EFF'S ORAL INTERVENTION DELIVERED BY KATITZA RODRIGUEZ
Fourth Session - 9 January to 20 January 2023

As delivered

Dear Madame Chair,

The Electronic Frontier Foundation would like to show its appreciation for the effort of the Ad-Hoc Secretariat in drafting the non-negotiating document and for facilitating the present session. EFF is also thankful for the opportunity to speak today and hopes we are given a meaningful opportunity to observe Member States' drafting negotiation process in the next few days, which can set a best practice precedent on effective and meaningful civil society participation. EFF looks forward to a fruitful discussion this week and next.

Our comments today will focus on Convention's proposed core cyber crimes (included in Cluster 1) as well as some other provisions that could undermine cyber security if left as proposed in the Consolidated Draft. To avoid duplication, we have also coordinated our comments with R3D and Derechos Digitales, We endorse their upcoming oral comments to this effect.

We note that EFF, R3D, and Derechos Digitales have joined more than 78 NGOs in more than 45 countries to raise serious concerns about the over expansive scope of the Convention as reflected in the Consolidated draft.

It is important to keep in mind that cyber crimes (including so-called 'core' cyber crimes) have been used to target journalists, political dissidents, whistleblowers, LGBTQ+ people, and good faith security researchers.

The Convention's core cyber-crime Articles, 6-10, therefore, should be narrowly scoped to avoid criminalization of legitimate conduct. Unfortunately, many of the Convention's core cyber crimes are expansively framed and will criminalize and chill important activities including activities protected by human rights. These provisions require amendments and detailed discussion.

Art. 6, 8, 9, and 10, for example, do not require fraudulent intent or actual harm and fail to include clear public interest exceptions. Nor are they limited to conduct that bypasses technical security safeguards without authorization. These provisions threaten to criminalize conduct on the basis that it violates an entity's contractual terms of use or internal security policies, effectively letting organizations determine the scope of criminal conduct. Collectively, these Articles are in dire need of amendment. Specifically:

- Article 6 might be used to criminalize conduct merely because it violates a contractual term of use or security policy, which some might consider 'unlawful.' Bypassing security protocols with malicious intent is only an *optional* component of this offense. Similar provisions have been used to silence whistleblowers and to attack critics of companies

and governments for merely posting hyperlinks to content that was already available online.

- Article 8 criminalizes any intentional and unlawful copying or downloading of digital information. Article 9 criminalizes "serious and unlawful" interference with computer systems or devices. Both Articles capture conduct even where no technical security safeguards have been bypassed. For example, these provisions could be used to criminalize copying of publicly available source code in violation of a service's terms of use by a social science researcher documenting algorithmic bias or a security researcher documenting a security breach, and could also capture a public interest advocacy group sending large volumes of unsolicited emails in a manner that slows down an email server. None of this conduct belongs in a criminal treaty.
- Article 10(1)(a)(ii) over-criminalizes password sharing. While passwords are sold criminally for profit, many more are shared by friends and family (without profit), which is more appropriately a civil issue if such action violates the company's Terms of Services. For example, Netflix, after years of ignoring password sharing, is now asking some of the hundreds of millions who share passwords to pay an additional $3.[1] As written, this Article could turn these millions of ordinary people into "cybercirminals" overnight. Thus such conduct should be excluded.
- Article 10(2) would limit the application of Article 10(1) to criminalizing possession and distribution for the purpose of committing an offence under proposed Articles 6-9 of the Convention, with the implication that doing so would remove criminal liability for authorized security testing or defensive conduct. Unfortunately, Articles 6-9 provide no clear protection for security testing. and as a result Article 10(1) threatens to criminalize the circulation and use of important security tools. Many tools are dual use in nature and, moreover, it is unclear how the circulation of malicious tools can be effectively criminalized while their circulation for cyber defense purposes is effectively excluded. The focus of Article 10(1) should unambiguously be on the specific use of tools for malicious purposes and Articles 6-9 should be clearly and unambiguously delimited to fraudulent and malicious conduct.

We urge Member States to re-assess the scope of these offenses. As currently framed, these provisions capture the important activity of public interest. History has shown that these provisions will be used to violate human rights, chill legitimate conduct, and counter-productively undermine the security of networks and devices.

[1] Kate O'Flaherty, *Netflix Password Sharing Alert—New Crackdown Starts In 2023*, Forbes (Dec 22, 2022) https://www.forbes.com/sites/kateoflahertyuk/2022/12/22/netflix-password-sharing-alert-new-crackdown-starts-in-2023/?sh=5964b59b7c41