Electronic Frontier Foundation Oral and Written Submission
Proposed Amendments to Clusters 1 and 2
January 12, 2023

The Electronic Frontier Foundation would like to signal its continued appreciation for the opportunity to provide input into the development of this Convention.

Proposed offenses in the Clusters 1 and 2 require additional safeguards, or they will criminalize and chill legitimate and publicly important activity and contravene human rights while counter-productively undermining security by prohibiting cyber defense.

As we noted in our earlier comments, Articles 6, 7, 8, and 10 of Cluster 1 and Arts. 11, 12 & 14 in Cluster 2 share four specific and recurring problems. To correct these, the draft should::

1. Add a clear statement ensuring that violations of internal access policies or company terms of service cannot form the basis for criminal liability.
    - [Provisions in Arts 6-9 require most prohibited conduct to be 'unlawful' in nature, and it must be clear that unlawfulness cannot turn on violations of private use policies or contractual arrangements. Civil disputes should not be criminalized. As currently framed, these provisions threaten to elevate private business disputes, based on contracts selected by companies, not legislatures, to criminal activity.]
2. Add a requirement of unauthorized intrusion onto networks or devices and define it as criminalizing conduct that results from bypassing technical security safeguards.
3. Add a requirement for prohibited conduct to be fraudulent in nature and have a 'harm' requirement.
    - [Core cyber crimes cast a wide net that can be used in many evolving technological contexts. It is therefore critical to ensure that only conduct that is intentionally fraudulent and that causes actual harm is criminalized.]
4. Add a recognition of the public interest. It is important to ensure that legitimate activity in the public interest is not criminalized by these provisions.
    - [There are many ways that this limitation can be achieved, and the specifics of what is required in national law to realize protection for these public interest impacts may change over time, but the principle that these provisions do not criminalize a range of public interest activity should be recognized in the text of the Convention.]

Absent these features, the Convention's criminal provisions remain problematic.

Madame Chair, a detailed explanation of how to draft the text requires more than three minutes. Therefore, we kindly submit a detailed analysis in written form, which we hope to be distributed to Member States.

Provision-Specific Examples

Article 6 might be used to criminalize conduct merely because it violates a contractual term of service or security policy, since some might consider such action '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 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.** This means that these provisions could be used to criminalize **copying of publicly available source code** that a social science researcher used in violation of a service's terms when documenting algorithmic bias in the ad industry or a security researcher documenting a security breach. 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. Netflix, for example, recently started 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 "cybercriminals" overnight. Thus such conduct should be excluded.

More generally, Article 10(1) would criminalize the possession, creation and dissemination of certain programs that could include key tools for cybersecurity testing. Article 10(2) would limit the scope of this criminal liability to situations where tools are created, possessed or distributed for the purpose of committing an offence under proposed Articles 6-9, with the intent of preventing the criminalization of security defence tools. Unfortunately, as outlined above and detailed in our earlier submissions, Articles 6-8 are framed too broadly and will criminalize legitimate cyber defence activities. By extension, Article 10(1) will continue to criminalize critical tools of cyber defence despite 10(2).

Even if issues with Articles 6-8 are cured, Article 10(1) remains problematic. Security tools are frequently dual use in nature. Even predominantly malicious tools are frequently used by security defence teams to probe internal networks and by security researchers more generally. It is unclear how the circulation of malicious tools can be effectively criminalized while their circulation for cyber defence purposes is effectively excluded. We would therefore ask that Article 10(1) apply primarily to the criminal and malicious use of tools, not to their possession or dissemination.

Article 14 of Cluster 2 similarly criminalizes legitimate security research by prohibiting the obtaining, use or dissemination of "information of any payment instrument". Article 14(c) also

---

[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

prohibits any “unauthorized access” to information pertaining to a payment system but fails to ensure that access cannot be prohibited on the basis of internal policies or terms of use documents. This provision could effectively prohibit security research including probing of publicly available open source payment systems and the circulation of information related to security flaws in those systems.[2]

Article 11 of Cluster 2 criminalizes intentional data alterations that result in inauthentic digital information for legal purposes. The provision permits but does not require the inclusion of a ‘fraudulent intent’ requirement. Altering or suppressing computer data is a common and legitimate forensic practice used by researchers documenting practices of websites and services in preparation for litigation.[3] We note more generally, the prohibition on fraudulently fabricating evidence is already inherent in any legal system that adheres to the rule of law, making this provision redundant to the extent they are not overbroad.

In contrast to other provisions in Clusters 1 and 2, Article 12 of Cluster 2 helpfully includes qualifiers such as “acts of fraud”, “loss of property” and “deceive or induce” which limit the scope of the provision. However, we are concerned that this provision may still be used against legitimate political advocacy. For example, it is common for parody accounts to use computer systems in order to advocate for companies to do things they might not otherwise do, often .

And finally, we note that Articles 13 and 14 criminalize conduct that is unambiguously already heavily criminalized such as theft and forgery.

We thank you again for the opportunity to provide input into this process and look forward to continuing to participate in the development of this Convention.

[2] https://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf.
[3] https://en.wikipedia.org/wiki/User_agent#Use_in_HTTP.