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

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, including the co-facilitated informal discussions in the next few days, which may set a best practice precedent on meaningful multi-stakeholder civil society participation.

Our comments today will focus on Convention's proposed core cyber crimes (included in Cluster 1). 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 '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 time for a detailed discussion.

Art. 6, 8, 9, and 10, for example, do not require fraudulent intent or actual harm. 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 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. 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 "cybercriminals" 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.

We urge Member States to engage in-depth debate over these provisions and 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.

R3D'S ORAL INTERVENTION DELIVERED BY GRECIA MACIAS
Fourth Session - 9 January to 20 January 2023

Red en Defensa de Los Derechos Digitales welcomes the opportunity to address the Ad-Hoc committee on the Consolidated Draft of a Cybersecurity treaty.

R3D appreciates the opportunity to speak today and the inclusion of civil society in this process. As my colleague from EFF stated, we have the opportunity to set a great precedent of open inclusion if stakeholders are allowed to be observers of the Member States drafting negotiation process, including co-facilitated informal discussions.

We will focus our comments today on the need to limit the criminal provisions of this treaty to true or core cybercrimes–that is, offenses against the confidentiality, integrity, and availability of computer data and systems. These provisions are primarily concentrated in Cluster 1 (Articles 6-10) and Cluster 2 (Articles 11-14) of the current Consolidated Draft.

---

[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

We'd also like to note that we endorse the recent comments delivered by our colleagues at EFF.

We would like to add that some of the Convention's offenses outside of Cluster 1 share problematic similarities to those discussed by EFF, with the effect of criminalizing digital conduct that is of public interest and protected by human rights standards. For example, Article 11, 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 forensic practice. For example, researchers documenting legal abuses on publicly available online services may alter the signal sent by their browser to emulate a different type of browser,[2] or modify their IP address to protect their privacy or see the geo-located content intended for a user based at another location.

More broadly, we note that any expansion of the scope of criminal conduct beyond core cybercrime offenses in this Convention poses a threat to human rights.

When enacting cybercrime laws, many states will criminalize online conduct related to public morality, posing a direct threat to the freedom of expression, the right to non-discrimination, and the right to privacy. By treating any conduct that occurs on digital networks as a potential 'cybercrime' (as per Clusters 2-10), the current draft legitimizes this problematic approach and encourages States to add their own list of public moral offenses when enacting their substantive criminal provisions into national law.

This is particularly a risk as the Cybercrime Convention does not advance any coherent conception or consensus of what does and does not constitute a 'cyber crime'.

We further believe that content-based crimes (crimes that prohibit the dissemination of online content) are particularly insidious to freedom of expression and should be categorically excluded from the Convention (Art. 23, 24-25, 26, 27, 28, 29).

Speech harms that are otherwise recognized as legally actionable do not need to be specially addressed as a criminal offense. Such speech is already carefully considered in other (non-cyber) contexts (terrorism, hate speech, genocide), where competing rights concerns between freedom of expression, privacy, and other rights have been carefully considered and accommodated.

Criminalization of "extremism-related" and "terrorism-related" offenses is particularly concerning, as these concepts have no clear and accepted definition in international law, and many States have historically relied on this lack of clarity to justify human rights abuses.

Finally, we have also coordinated our comments with my colleague from Derechos Digitales and endorsed them.

---

[2] https://en.wikipedia.org/wiki/User_agent#Use_in_HTTP.

DERECHOS DIGITALES'S ORAL INTERVENTION DELIVERED BY MARIA PAZ CANALES
Fourth Session - 9 January to 20 January 2023

Dear Madame Chair,

Derechos Digitales welcomes the opportunity to contribute in this Fourth Session of the Ad Hoc Committee, and thanks the Chair for her leadership in drafting the consolidated negotiating document and for facilitating the present session.

Derechos Digitales welcomes the opportunity to speak today and look forward for the opportunity to observe Member States' drafting negotiation process, including the co-faciliated informal discussions this week and the next, in order to continue allowing civil society participation and the possibility to meaningfully contribute and collaborate with States in this difficult task at hand.

In seeking to negotiate the proposed consolidated negotiating document over the next two weeks, we hope the evolving text will only contain criminal offenses that reflect a consensus among Member States and, in particular, that the final text is limited to core cybercrimes.

We join our colleagues at EFF and R3D in the view that proposed offenses in Articles 11 to 34 included solely on the basis that technology is used in their commission, "or cyber enabled", should be excluded from the Convention and that their inclusion threatens human rights.

Our comments will address proposed offenses in the consolidated negotiating document that should be excluded on the basis that they interfere with the right to freedom of expression or because they receive more nuanced treatment in other contexts and particularly in contexts that are more focused on civil, administrative and regulatory solutions.

We note that much of the conduct in Articles 11 to 22 (Clusters 2-6) in particular is already largely and more effectively addressed in other contexts, frequently with more nuanced treatment and with reliance on more appropriate civil or regulatory remedies.

For example, as pointed out in Article 19's written submission to this Committee, 179 Member States are already parties to the Protocol to the Convention of the Rights of the Child, where mutual assistance already exists. Therefore, we question the need for inclusion of Articles 18-21 of the consolidated negotiating document.

Copyright enforcement is also addressed in numerous other contexts with greater nuance and is primarily a civil or administrative matter. Article 17 lacks this nuance. It makes no mention, for example, of the importance of copyright flexibilities (fair dealing/use exceptions) that are critical to ensuring protections remain balanced and consistent with human rights obligations such as the freedom of expression and access to knowledge. Article 17 would also seemingly elevate to

criminal status (subject to explicit reservation under Article 17.3) the willful infringement on a commercial scale of *any* copyright protection adopted in any other convention a State Party might have acceded to, ignoring the careful balancing between criminal and other protections explicitly adopted in those conventions.

The protection of personal information is critically important, but its treatment as a purely criminal offense as proposed in the consolidated negotiating document also lacks the nuance necessary for effective and properly tailored protection of privacy. Article 15 criminalizes any intentional and unlawful access to or distribution of personal information with the intent of obtaining a financial benefit and without consent. Article 15 provides no latitude for important nuances such as the disclosure of personal information without consent in news articles, and newspapers are often legally viewed as circulated for the purpose of financial profit.

Finally, we further note that offenses in Articles 30-34 occur at least as much in the physical world as in the digital. Creating a parallel enforcement and cooperation regime that is focused solely on the digital aspect of these problems is unnecessary and could even undermine existing global enforcement efforts.

We thank the Ad Hoc Committee for providing us with an opportunity to voice these concerns and look forward to engaging with the Committee further as the drafting process continues.

ETICAS FOUNDATION ORAL INTERVENTION DELIVERED BY TANJA FACHATHALER
Fourth Session - 9 January to 20 January 2023

Thank you Madam Chair, Honourable Representatives,

Eticas Foundation appreciates the effort of the Ad-Hoc-Working Group, its members and staff for the drafting of the CND, for facilitating the present session and for ensuring that the elaboration of a Cybercrime Convention is an all-inclusive process**, which includes civil society**.

Having said this, please allow me to highlight the open letter signed by 79 NGOs from more than 45 countries that raise alarm about the human rights implications of the current draft of the treaty under negotiation.

Today, I am delighted to speak in this forum as **a** representative on behalf of Eticas Foundation and I look forward to the upcoming days of discussion and exchange.

In our opinion and highlighted by many representatives in yesterday's sessions as well as this morning, the scope of the criminalised offenses in the CND is overly broad and creates redundancies with existing international instruments.

This, in turn, leads to legal uncertainty, is harmful for core rights like the freedom of expression and risks establishing a dual legal standard.

Cybercrimes should indeed be understood as offenses where ICT systems are the direct objects and instruments of the crime.

We therefore suggest limiting the scope of the treaty to the core cybercrims of Cluster 1 (Articles 6 – 10) and to remove the remaining clusters on criminalisation (Clusters 2 – 10) from the negotiating text all together.

If, however, other non-cyber-dependent crimes were to be included, such cyber-enabled crimes should be narrowly defined and consistent with international human rights standards.
Having said this, we are very concerned about the inclusion of content-related offenses (Clusters 4,7,8,9). Their inclusion poses a high risk that **the** Convention will be used to prohibit expression that is protected under international human rights standards and the clusters should therefore not be included in the draft Convention.

Also, we are very concerned about inclusion of „extremism-related offenses“ (Article 27) and „terorism-related offenses“ (Article 29). There are no agreed international definitions for these crimes and keeping them in the text may justify human rights repressive practices like the prosecution of political opponents, human rights defenders or journalists, as well as the unlawful restriction of the exercise of the rights of freedom of expression and peaceful assembly or the unlawful interference with the right to privacy.

These provisions should not serve as a basis to restrict core rights and freedoms and hence should be removed under all circumstances.

We all share the aim of a trustworthy digital environment that respects human rights. But this can only be achieved if this Convention is narrow in scope and does not criminalise the central practice of responsible disclosure in order to protect the vital work of security researchers, journalists or whistleblowers – acting in good faith.

It is therefore crucial that the criminalisation provisions be amended and a standard of fraudulent intent and harm be introduced so as to avoid the criminalisation of legitimate conduct.
Madam Chair, we hope to continue the discussion on these issues and remain available for further input on the individual provisions during the negotiations.

Thank you.

Global Partners Digital
Thank you Chair, distinguished delegates, for the opportunity to provide our perspectives on the consolidated negotiating document or CND. Global Partners Digital is a civil society organisation, working globally to support a digital environment underpinned by human rights.
We have been following this process from its onset, and provided contributions aimed at ensuring that the convention is aligned with international human rights law and standards.

In our most recent contribution relating to the CND, available online, we provide our analysis and related recommendations on each of the chapters under discussion here.

As many delegations have noted, there is limited time and the only way to have effective discussions is to focus on areas where there is agreement and where consensus could be found. It is also imperative that the convention upholds international human rights obligations. Moreover, it is important to avoid duplication - and even the risk of misalignment - with existing instruments, as has also been noted multiple times.

Therefore, regarding criminalisation, our recommendations are as follows.

● The scope of criminal offences should be restricted to a core set of cybercrimes–cyber-dependent crimes - criminal offences in which information and communications technology (ICT) systems are the direct objects, as well as instruments, of the crimes–including only those offences listed in Cluster 1 of the consolidated text and narrowly scoped to avoid criminalization of legitimate conduct.
● To that end, Articles 6 to 10 should be amended to include a standard of malicious/ fraudulent intent and harm, or provide a more clearly articulated and expansive public interest defence.
● Should further offences be included beyond core cybercrimes, these must reflect international consensus and should be narrowly defined and strictly consistent with international human rights standards.
● Content-related offences, including those in Clusters 4, 7, 8 and 9, should be removed.

Finally, GPD has also signed onto a joint letter and analysis, published on the AHC website, which has a growing list of civil society signatories - currently at 79 from more than 45 countries around the world.

The principle of meaningful participation requires that stakeholders are permitted to participate in informal consultations, not least because the object of these consultations is to “explore possibilities to achieve consensus on specific challenging areas.” The discussion of challenging and contentious in particular necessitates the observation of and input by multi-stakeholders.