Civil Society Letter on the Proposed Cybercrime Treaty

H.E. Ms. Faouzia Boumaiza Mebarki

Chairperson

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes

Your Excellency:

We, the undersigned organizations and academics, work to protect and advance human rights, online and offline. Our collective goal is to ensure that human rights and fundamental freedoms are always prioritized when countering cybercrime, securing electronic evidence, facilitating international cooperation, or providing technical assistance. While we are not convinced that a global cybercrime convention is necessary, we would like to reiterate the need for a human-rights-by-design approach in the drafting of the proposed UN Cybercrime Convention.

We have grave concerns that the draft text released by the committee on November 7, 2022, formally entitled "the consolidated negotiating document (CND) on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes," risks running afoul of international human rights law.

The CND is overbroad in its scope and not restricted to core cybercrimes. The CND also includes provisions that are not sufficiently clear and precise, and would criminalize activity in a manner that is not fully aligned and consistent with States' human rights obligations set forth in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and other international human rights standards and instruments.[1] Further, the CND's criminal procedural and law enforcement chapter lacks robust human rights safeguards, while its substantive provisions expand the scope of criminal intent and conduct, threatening to criminalize legitimate activities of journalists, whistleblowers, security researchers, and others.

Failing to prioritize human rights throughout all the Chapters can have dire consequences. The protection of fundamental rights has consistently been raised by Member States throughout the sessions of the Ad Hoc Committee to elaborate the Proposed Convention. Many States and

[1] These instruments are the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social, and Cultural Rights (ICESCR), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Convention on the Elimination of All Forms of Racial Discrimination (CERD), the Convention on the Rights of the Child (CRC), among other international and regional human rights instruments and standards).

non-governmental stakeholders have called for the Proposed Convention to be fully aligned and consistent with international human rights law. Any permitted measures restricting rights need to be prescribed by law, justified on legal grounds permitted strictly in relation to the rights concerned, and be necessary and proportionate to pursue a legitimate objective. Provisions should also respect the rule of law by including sufficient specificity and independent oversight to ensure their implementation aligns with their intended scope. So, it's extremely troubling to see that many provisions in the CND are drafted in a way that does not uphold human rights law, in substance or in process, and open the door to implementation in ways that threaten further violations of human rights and the rule of law.

Specifically, we are concerned that CLUSTERS 2 to 10 include a long list of offences that are not core cybercrimes, offences that interfere with protected speech and fail to comply with permissible restrictions under international freedom of expression standards, or offences drafted with vague or overbroad language.

The Criminalization Chapter should be restricted to core cybercrimes–criminal offences in which information and communications technology (ICT) systems are the direct objects, as well as instruments, of the crimes; these crimes could not exist at all without the ICT systems. A useful reference for the types of crimes that are inherently ICT crimes can be found in Articles 2-6 of the Budapest Convention. Should other non-core cybercrimes be included, we recommend that those "cyber-enabled" crimes be narrowly defined and strictly consistent with international human rights standards.

Crimes, where ICT systems are simply a tool that is sometimes used in the commission of an offence, should be excluded from the proposed Convention. These would include crimes already prohibited under existing domestic legislation and merely incidentally involving or benefiting from ICT systems without targeting or harming those systems, as in some of the crimes under CLUSTERS 2 and 10.

We are particularly concerned about the inclusion of content crimes such as "extremism-related offences" (Article 27) and "terrorism-related offences" (Article 29). These provisions disregard existing human rights standards set out by various UN bodies on policies and national strategies to counter and prevent terrorism and violent extremism. In particular, freedom of expression mandates holders have reiterated that broad and undefined concepts such as "terrorism" and "extremism" should not be used as a basis to restrict freedom of expression. In addition, there are no uniform definitions of these concepts in international law, and many States rely on this ambiguity to justify human rights abuses such as politically-motivated arrests and prosecutions of civil society members, independent media, and opposition parties, among others.

More generally, the inclusion of several content-related offences is profoundly concerning (as in some of the crimes under CLUSTERS 4, 7, 8, and 9). As we have reiterated throughout the negotiating process, this instrument should not include speech related offences. Including these crimes poses a heightened risk that the proposed Convention will contravene existing

international protection of freedom of expression and be used to restrict protected expression under international human rights standards.

Moreover, core cybercrime offences under CLUSTER 1 would impose some restrictions that might interfere with the essential working methods of journalists, whistleblowers, and security researchers and needs to be revised. Articles 6 and 10, for example, should also require a standard of both fraudulent intent and harm - a requirement that many delegations suggested as essential to consider during the discussion on this issue in the second substantive session.

The provisions on the Convention's procedural powers also raise concerns. Investigative powers required by the Convention should only be available with respect to crimes covered by the Convention. The Convention concerns cybercrime and should not become a general purpose vehicle to investigate any and all crimes.

While the general obligation to respect the principles of proportionality, necessity, and legality and the protection of privacy and personal data in implementing procedural powers is welcome, additional specificity is necessary to ensure human rights are respected in the implementation of the Convention. To that effect, Article 42 should specify that prior independent (preferably judicial) authorization and independent ex-post monitoring are required, recognize the need for effective remedies, require rigorous transparency reporting and user notification by state parties, and include guarantees to ensure that any investigative powers do not compromise the integrity and security of digital communications and services.

The Convention's procedural mechanisms should also ensure that international law and human rights standards with respect to evidence are respected. Evidence obtained in violation of domestic law or of human rights should be excluded from criminal proceedings as should any further products of that evidence.

The Convention's preservation powers (Articles 43 and 44) should ensure that preservation requirements and renewals are also premised on reasonable belief or suspicion that a criminal offence has or is being committed and that the data sought to be preserved will yield evidence of that offence. The preservation period should not exceed sixty (60) days, subject to renewal, and the Convention should clarify that national laws requiring preservation in excess of the specified period will not qualify for implementation. Article 43 should further specify that service providers are required to expeditiously delete any preserved data once the preservation period ends.

Article 46(4) raises serious concerns vis-a-vis the potential obligations imposed upon third parties, such as service providers, to either disclose vulnerabilities of certain software or to provide relevant authorities with access to encrypted communications.

Article 47 on a real-time collection of traffic data should be revised and written in a more precise way to ensure that the Article does not authorize any blanket or indiscriminate data

retention measures. The generalized interception, storage, or retention of the content of communications or its metadata has been deemed to have failed the necessary and proportionate test.[2]

Articles 47 and 48 should be amended to clarify that they do not include state hacking of end devices. State hacking powers remain controversial and can cause collateral harm to the integrity and security of networks, data, and devices. There is no consensus as to when these powers can be appropriately invoked, and there is a risk that some State Parties will inappropriately implement Articles 47 and 48 to include this type of intrusive surveillance.

The Convention's confidentiality provisions (Articles 43(3), 47(3), and 48(3)) should only apply to the extent necessary to prevent any threats to investigations that might ensue in the absence of confidentiality.

We respectfully recommend that the CND be revised to ensure that:

- The scope of the Convention should be limited to issues within the realm of the criminal justice system and should be limited in both its substantive and procedural scope to core cyber crimes.
- The proposed crimes under Articles 6 and 10 should be revised to include, at minimum, a standard of both fraudulent intent and harm, to protect journalists, whistleblowers, and security researchers [CLUSTER 1].
- The criminalization chapters should be restricted to offences against the confidentiality, integrity, and availability of computer data and systems.
- Crimes where ICTs are simply a tool that is sometimes used in the commission of an offence should be excluded from the proposed Convention. [CLUSTERS 2-10]
- Should other non-core cybercrimes be included, we recommend that those cyber-enabled crimes are narrowly defined and consistent with international human rights standards, and, in any case, no speech offences should be included.
- Any criminal offences that restrict activity in a manner that is inconsistent with human rights law should be excluded. The risk that an overbroad list of online content, speech, and other forms of expression may be considered a cybercrime under the proposed Convention is a major concern that should be addressed, particularly through the removal of any content offences [See CLUSTERS 4, 7, 8, and 9].
- Investigative powers in Criminal Procedural Measures and Law Enforcement Chapter III should be carefully scoped so that they remain closely linked to investigations of specific criminal conduct and proceedings and should only be available for investigations of crimes specifically covered by the Convention (Article 41(2)).
- Secrecy provisions should only be available where disclosure of the information in question would pose a demonstrable threat to an underlying investigation (Articles 43(3), 47(3), and 48(3).

[2] https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

- When it comes to criminal procedural measures, any proposed obligations that enable investigation and prosecution should come with detailed and robust human rights safeguards and rule of law standards, including a requirement for independent oversight and control and the right to an effective remedy.
- General provisions authorizing interception and real time collection of data should be amended to clarify that they do not authorize intrusion into networks and end devices. These provisions lack sufficient safeguards to address the threat to the security and integrity of networks, data, and devices posed by state hacking, and State Parties should not be able to rely on ambiguities in the text to justify hacking activities (Articles 47 and 48).
- The text should not authorize any indiscriminate or indefinite retention of metadata.

Negotiating an international cybercrime Convention with Member States is not an easy task. But it is paramount that this Convention, which has the potential to profoundly impact millions of people around the world, makes it crystal clear that fighting global cybercrime should reinforce and not endanger or undermine human rights.

Submitted by NGOS registered under operative 8 or 9.

- Red en Defensa de los Derechos Digitales - Mexico
- Access Now - International
- Association for Progressive Communications (APC) - International
- Center for Democracy and Technology (CDT) - International
- Data Privacy Brasil - Brazil
- Derechos Digitales - Latin America
- Eticas Data Society Foundation - International
- Fundacion Via Libre - Argentina
- Human Rights Watch - International
- Hiperderecho - Perú
- IPANDETEC - Central America

The full list of signatories supporter of the letter is available on this link.