Urgent Appeal to Address Critical Flaws in the Latest Draft of the UN Cybercrime Convention

Ahead of the reconvened concluding session of the United Nations (UN) Ad Hoc Committee on Cybercrime (AHC) in New York later this month, we, the undersigned organizations, wish to urgently draw your attention to the persistent critical flaws in the latest draft of the UN cybercrime convention (hereinafter Cybercrime Convention or the Convention).

Despite the recent modifications, we continue to share profound concerns regarding the persistent shortcomings of the present draft and we urge member states to not sign the Convention in its current form.

Key concerns and proposals for remedy:

1. Overly Broad Scope and Legal Uncertainty:

- The draft Convention's scope remains excessively broad, including cyber-enabled offenses and other content-related crimes. The proposed title of the Convention and the introduction of the new Article 4 – with its open-ended reference to "offenses established in accordance with other United Nations conventions and protocols" – creates significant legal uncertainty and expands the scope to an indefinite list of possible crimes to be determined only in the future. This ambiguity risks criminalizing legitimate online expression, having a chilling effect detrimental to the rule of law. We continue to recommend **narrowing the Convention's scope to clearly defined, already existing cyber-dependent crimes only, to facilitate its coherent application, ensure legal certainty and foreseeability and minimize potential abuse**.
- The draft Convention in **Article 18 lacks clarity concerning the liability of online platforms** for offenses committed by their users. The current draft of the Article lacks the **requirement of intentional participation** in offenses established in accordance with the Convention, thereby also contradicting Article 19 which does require intent. This poses the risk that online intermediaries could be held liable for information disseminated by their users, even without actual knowledge or awareness of the illegal nature of the content (as set out in the EU Digital Services Act), which will incentivise overly broad content moderation efforts by platforms to the detriment of freedom of expression. Furthermore, the wording is much broader ("for participation") than the Budapest Convention ("committed for the cooperation's benefit") and would merit clarification along the lines of paragraph 125 of the Council of Europe Explanatory Report to the Budapest Convention.
- The proposal in the revised draft resolution to elaborate a draft protocol supplementary to the Convention represents a further push to expand the scope of offenses, risking the creation of a limitlessly expanding, increasingly punitive framework.

2. Insufficient Protection for Good-Faith Actors:

- The draft Convention fails to incorporate language sufficient to protect good-faith actors, such as security researchers (irrespective of whether it concerns the authorized testing or protection of an information and communications technology system), whistleblowers, activists, and journalists, from excessive criminalization. It is crucial that the mens rea element in the provisions relating to cyber-dependent crimes includes **references to criminal intent and harm caused**.

3. Lack of Specific Human Rights Safeguards:

- Article 6 fails to include specific human rights safeguards – as proposed by civil society organizations and the UN High Commissioner for Human Rights – to ensure a common understanding among Member States and to facilitate the application of the treaty without unlawful limitation of human rights or fundamental freedoms. These safeguards should be:
    - **applicable to the entire treaty** to ensure that cybercrime efforts provide adequate protection for human rights;
    - be in accordance with the **principles of legality, necessity, and proportionality, non-discrimination, and legitimate purpose**;
    - incorporate the **right to privacy** among the human rights specified;
    - address the lack of effective **gender mainstreaming** to ensure the Convention does not undermine human rights on the basis of gender.

4. Procedural Measures and Law Enforcement:

- The Convention should **limit the scope of procedural measures** to the investigation of the criminal offenses set out in the Convention, in line with point 1 above.
- In order to facilitate their application and – in light of their intrusiveness – to minimize the potential for abuse, this chapter of the Convention should incorporate the following minimal **conditions and safeguards** as established under **international human rights law.** Specifically, the following should be included in **Article 24**:
    - the principles of legality, necessity, proportionality, non-discrimination and legitimate purpose;
    - prior independent (judicial) authorization of surveillance measures and monitoring throughout their application;
    - adequate notification of the individuals concerned once it no longer jeopardizes investigations;
    - and regular reports, including statistical data on the use of such measures.

- **Articles 28/4, 29, and 30 should be deleted**, as they include excessive surveillance measures that open the door for interference with privacy without sufficient safeguards as well as potentially undermining cybersecurity and encryption.

5. International Cooperation:

- The Convention should limit the scope of international cooperation solely to the crimes set out in the Convention itself to avoid misuse (as per point 1 above.) Information sharing for law enforcement cooperation should be limited to specific criminal investigations with explicit data protection and human rights safeguards.
- Article 40 requires “the widest measure of mutual legal assistance” for offenses established in accordance with the Convention as well as any serious offense under the domestic law of the requesting State. Specifically, where no treaty on mutual legal assistance applies between State Parties, paragraphs 8 to 31 establish extensive rules on obligations for mutual legal assistance with any State Party with generally insufficient human rights safeguards and grounds for refusal. For example, paragraph 22 sets a high bar of ”substantial grounds for believing” for the requested State to refuse assistance.
- When State Parties cannot transfer personal data in compliance with their applicable laws, such as the EU data protection framework, the conflicting obligation in Article 40 to afford the requesting State “the widest measure of mutual legal assistance” may unduly incentivize the transfer of the personal data subject to appropriate conditions under Article 36(1)(b), e.g. through derogations for specific situations in Article 38 of the EU Law Enforcement Directive. Article 36(1)(c) of the Convention also encourages State Parties to establish bilateral and multilateral agreements to facilitate the transfer of personal data, which creates a further risk of undermining the level of data protection guaranteed by EU law.
- When personal data is transferred in full compliance with the data protection framework of the requested State, Article 36(2) should be strengthened to include clear, precise, unambiguous and effective standards to protect personal data in the requesting State, and to avoid personal data being further processed and transferred to other States in ways that may violate the fundamental right to privacy and data protection.

Conclusion and Call to Action:

Throughout the negotiation process, we have repeatedly pointed out the risks the treaty in its current form pose to human rights and to global cybersecurity. Despite the latest modifications, the revised draft fails to address our concerns and continues to risk making individuals and institutions less safe and more vulnerable to cybercrime, thereby undermining its very purpose.

Failing to narrow the scope of the whole treaty to cyber-dependent crimes, to protect the work of security researchers, human rights defenders and other legitimate actors, to strengthen the human rights safeguards, to limit surveillance powers, and to spell out the data protection principles will give governments' abusive practices a veneer of international legitimacy. It will also make digital communications more vulnerable to those cybercrimes that the Convention is meant to address. Ultimately, if the draft Convention cannot be fixed, it should be rejected.

With the UN AHC's concluding session about to resume, we call on the delegations of the Member States of the European Union and the European Commission's delegation to redouble their efforts to address the highlighted gaps and ensure that the proposed Cybercrime Convention is narrowly focused in its material scope and not used to undermine human rights nor cybersecurity. Absent meaningful changes to address the existing shortcomings, we urge the delegations of EU Member States and the EU Commission to reject the draft Convention and not advance it to the UN General Assembly for adoption.

This statement is supported by the following organizations:

Access Now
Alternatif Bilisim
ARTICLE 19: Global Campaign for Free Expression
Centre for Democracy & Technology Europe
Committee to Protect Journalists
Digitalcourage
Digital Rights Ireland
Digitale Gesellschaft
Electronic Frontier Foundation (EFF)
epicenter.works
European Center for Not-for-Profit Law (ECNL)
European Digital Rights (EDRi)
Global Partners Digital
International Freedom of Expression Exchange (IFEX)
International Press Institute
IT-Pol Denmark
Media Policy Institute (Kyrgyzstan)
Privacy International
SHARE Foundation
Vrijschrift.org
World Association of News Publishers (WAN-IFRA)
Zavod Državljan D (Citizen D)