

Open Letter from Civil Society and Industry Stakeholders on the Final Draft of the Convention on Cybercrime

August 8, 2024

Your Excellency,

The undersigned stakeholders stand united in urging governments not to adopt or ratify the UN's first landmark Cybercrime Convention unless substantial changes are made to address the serious and broad-based concerns in the final draft.

Our group, which includes civil society, industry, and the technical community, is united in our profound concerns over critical shortcomings in the final text that may be adopted this week. The final draft contains ambiguous provisions and definitions related to criminalization, and lacks sufficient respect and protections for human rights, press freedom, and gender equality, thereby endangering a range of groups. We would like to urgently draw your attention to serious flaws that our communities have repeatedly identified. Without effectively addressing all of the below issues we call on member states not to adopt the Convention.

Scope and Title of the Convention: We are alarmed by the unclear and overly broad scope of the Convention, particularly regarding its criminalization, procedural measures, and international cooperation chapters. We urge states to narrow the focus solely on cybercrime – those offences specifically provided for in the criminalization chapter – and amend the title to address only cybercrime, i.e., attacks on computer systems.

Human Rights Safeguards: It is crucial to maintain robust human rights safeguards in the final text, including existing references to gender. We call on states to ensure these safeguards are upheld, as follows: retain Article 6 as provided in the third revision; and replace “chapter” with “convention” in 24.1 and 24.4. We believe it is imperative that powers and procedures provided for by the Convention are exercised in accordance with States’ obligations under international human rights law. Article 24 should be amended to ensure it incorporates international human rights principles, particularly legality and necessity, and be subject to independent prior authorisation and review. Article 6 should include references to specific international frameworks, such as the International Covenant on Civil and Political Rights (ICCPR), to ensure that actions against cybercrime conform to established human rights standards. Article 35 urgently requires a mandatory dual criminality measure, an explicit human rights safeguards provision, and a prohibition on mutual legal assistance in cases where there are credible reasons to believe that the request is politically motivated or arbitrary, as proposed by Costa Rica and supported by a majority of member states.

Risks of overreach and abuse: The current text allows States to cooperate in permanent secrecy, which is not consistent with the rule of law, and has very expansive real-time interception powers to investigate and cooperate on a wide range of crimes. This in turn facilitates secret access to secured systems, extraterritorial exfiltration of data, and secret real-time data collection. A Convention containing such an unprecedented combination of powers, absent sufficient and robust conditions and safeguards, would present grave risks to human rights, individual safety, security and privacy, as well as potentially to national

security. We call on states to limit the scope to only those powers that are lawful, necessary and proportionate for the purpose of legitimate measures addressing cybercrime.

Protection of Cybersecurity Experts, Journalists, Activists, Whistleblowers and others: The Convention fails to protect cybersecurity experts and researchers who play an important role in securing ICTs from criminal activity by detecting and investigating security vulnerabilities. It also would allow others engaged in manifestly beneficial activities to be prosecuted, such as journalists and whistleblowers. We call on states to ensure these vital communities are effectively protected from prosecution.

Unless substantial changes are included to the final draft Convention to address these broad-based and fundamental concerns, we urge governments not to adopt the treaty, and if it is adopted, not to ratify it.

Signatories:

- AccessNow
- C4 Recovery Foundation
- Cybersecurity Tech Accord
- Electronic Frontier Foundation (EFF)
- epicenter.works - for digital rights
- Global Partners Digital (GPD)
- Knowmad institut
- International Press Institute (IPI)
- Misión Sacerdotal, sva
- Red en Defensa de los Derechos Digitales