UN Cybercrime Convention must not become a tool to undermine international human rights standards

Signatories stress that the Convention should only move forward if it pursues a specific goal of combating cybercrime without endangering the human rights and fundamental freedoms of those it seeks to protect, nor undermining efforts to improve cybersecurity for an open internet.

Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session

We, the undersigned organizations [and individual experts] call on the state delegations participating in the concluding session of the United Nations (UN) Ad Hoc Committee to ensure that the proposed Cybercrime Convention (the Convention) is narrowly focused on tackling cybercrime, and not used as a tool to undermine human rights. Absent meaningful changes to address these shortcomings, the Convention should be rejected.

Civil society groups have contributed time and expertise to improve the draft and fully align it with existing human rights law and standards, the principles of the UN Charter and the rule of law, as well as best practices to provide legal certainty in efforts to improve cybersecurity. Our concerns about the proposed text of the Convention are informed by our experience and human rights advocacy around the world. National and regional cybercrime laws are regrettably far too often misused to unjustly target journalists and security researchers, suppress dissent and whistleblowers, endanger human rights defenders, limit free expression, and justify unnecessary and disproportionate state surveillance measures.

Throughout the negotiations over the last two years, civil society groups and other stakeholders have consistently emphasized that the fight against cybercrime must not come at the expense of human rights, gender equality, and the dignity of the people whose lives will be affected by this Convention. It should not result in impeding security research and making us all less secure. Robust and meaningful safeguards and limitations are essential to avoid the possibility of abuse of relevant provisions of the Convention that could arise under the guise of combating cybercrime. Regrettably, the **latest draft** of the proposed Convention, which is due to be finalized by February 2024, fails to address many of our significant concerns. We believe that if the text of the Convention is approved in its current form, the risk of abuses and human rights violations will increase exponentially and leave us with a less secure internet.

We are particularly concerned that the latest draft of the Convention:

- Remains over-broad in the scope of the range of the activities it requires states to criminalize. It includes cyber-enabled offenses and other content-related crimes and creates legal uncertainty through an open-ended reference to crimes under other "applicable international conventions and protocols." This overbroad scope gives rise to the danger that the Convention will be used to criminalize legitimate online expression, which is likely to create discriminatory impacts and deepen gender inequality;
- Fails to incorporate language sufficient to protect security researchers, whistleblowers, activists, and journalists from excessive criminalization;
- Contains insufficient references to states' obligations under international human rights law, includes weak domestic human rights safeguards in its criminal procedural chapter, and fails to explicitly incorporate robust safeguards applicable to the whole treaty to ensure that cybercrime efforts provide adequate protection for human rights and are in accordance with the principles of legality, non-discrimination, legitimate purpose, necessity, and proportionality;
- Lacks effective gender mainstreaming which is critical to ensure the Convention is not used to undermine people's human rights on the basis of gender;
- Proposes to create legal regimes to monitor, store, and allow cross-border sharing of information in a manner that would undermine trust in secure communications and infringe on international human rights standards, including the requirements for prior judicial authorization and the principles of legality, non discrimination, legitimate purpose, necessity, and proportionality;
- Permits excessive information sharing for law enforcement cooperation, beyond the scope of specific criminal investigations and without specific, explicit data protection and human rights safeguards.

The Convention should only move forward if it pursues a specific goal of combating cybercrime without endangering the human rights and fundamental freedoms of those it seeks to protect nor undermining efforts to improve cybersecurity for an open internet. The present draft text falls far short of this goal and these basic minimum requirements, and must be comprehensively revised, amended, or rejected.

Therefore, we call on all state delegations to:

- Narrow the scope of the whole Convention to cyber-dependent crimes specifically defined and included in its text;
- Make certain the Convention includes provisions to ensure that security researchers, whistleblowers, journalists, and human rights defenders are not prosecuted for their legitimate activities and that other public interest activities are protected;
- Guarantee that explicit data protection and human rights standards – including the principles of non-discrimination, legality, legitimate purpose, necessity and proportionality – are applicable to the whole Convention. Specific, explicit safeguards, such as the principle of prior

judicial authorization, must be put in place for accessing or sharing data, as well as for conducting cross-border investigations and cooperation in accordance with the rule of law;
- Mainstream gender across the Convention as a whole and throughout each article in efforts to prevent and combat cybercrime;
- Limit the scope of application of procedural measures and international cooperation to the cyber-dependent crimes established in the criminalization chapter of the Convention;
- Avoid endorsing any surveillance provision that can be abused to undermine cybersecurity and encryption.

As the UN Ad Hoc Committee convenes its concluding session, we call on state delegations to redouble their efforts to address these critical gaps in the current draft. The final outcome of the treaty negotiation process should only be deemed acceptable if it effectively incorporates strong and meaningful safeguards to protect human rights, ensures legal clarity for fairness and due process, and fosters international cooperation under the rule of law. The proposed Convention must not serve as a validation of intrusion and surveillance practices harmful to human rights.

Absent these minimum requirements, we call on state delegations to reject the draft treaty and not advance it to the UN General Assembly for adoption.

Submitted by NGOS registered under operative paragraphs 8 or 9

Access Now
Association for Progressive Communications (APC)
ARTICLE 19
Center for Democracy and Technology
CyberPeace Institute
Data Privacy Brasil
Derechos Digitales
Electronic Frontier Foundation
Freedom House
Global Partners – Digital
Hiperderecho
Human Rights Watch
Instituto Panamericano de Derecho y Tecnologia (IPANDETEC)
International Commission of Jurists (ICJ)
Jokkolabs Banjul
Jonction – Senegal
Kenya ICT Action Network (KICTANet)
Privacy International

R3D: Red en Defensa de los Derechos Digitales
Temple University, Institute for Law, Innovation & Technology (iLIT)

Full list of signatories supporting the letter

7amleh – The Arab Center for the Advancement of Social Media
ActiveWatch
Advocacy for Principled Action in Government
Afghanistan Journalists Center (AFJC)
Africa Freedom of Information Centre (AFIC)
AfroLeadership
Albanian Media Institute
Alliance of Independent Journalists Indonesia (AJI)
Alternatif Bilisim (AiA-Alternative Informatics Association)
Alternative ASEAN Network on Burma (ALTSEAN)
Bahrain Center for Human Rights
Bangladesh NGOs Network for Radio & Communication (BNNRC)
BC Civil Liberties Association (BCCLA)
Bytes for All
Cambodian Center for Human Rights (CCHR)
Cambodian Centre for Independent Media (CCIM)
Cartoonists Rights Network International
Center for Media Freedom and Responsibility
Centre for Feminist Foreign Policy (CFFP)
Centre for Free Expression (CFE)
Centre for Information Technology and Development (CITAD)
Centre for Independent Journalism (Malaysia)
Chaos Computer Club (CCC)
Committee to Protect Journalists
Douwe Korff, Emeritus Professor of International Law, London Metropolitan University
Digital Empowerment Foundation
DigitalReach
Digital Rights Foundation
Digital Rights Ireland
Digitale Gesellschaft
Electronic Privacy Information Center (EPIC)
Epicenter.works – for digital rights
European Center for Not-for-Profit Law (ECNL)
European Digital Rights (EDRi)
European Summer School in Internet Governance (EURO-SSIG)

Federation of Nepali Journalists
Foundation for Media Alternatives
Fundación Karisma
Fundación Internet Bolivia
Foundation for Information Policy Research
Freedom Forum, Nepal
Free Media Movement – Sri Lanka
Globe International Center
Government Information Watch
Gulf Center for Human Rights (GCHR)
Human Rights Network for Journalists-Uganda (HRNJ-U)
IFoX (Initiative for Freedom of Expression–Turkey)
Independent Journalism Center Moldova
International Civil Liberties Monitoring Group (ICLMG)
International Federation of Human Rights (FIDH)
International Press Institute (IPI)
International Press Centre (IPC) Lagos-Nigeria
Institute for Research on Internet and Society (IRIS)
Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec
Instituto Nupef
IT-Pol Denmark
Japan Comuter Access Network (JCA-NET)
Jinbonet (Korean Progressive Network Center)
Laboratory of Public Policy and Internet – LAPIN
LaLibre.net Tecnologías Comunitarias
Ligue des droits de l'Homme (LDH)
Maharat Foundation
Media Foundation for West Africa (MFWA)
Media Rights Agenda (MRA)
Media Institute of Southern Africa (MISA)
Media Policy Institute
Media Watch
Metamorphosis Foundation
Mizzima
OpenMedia
Pakistan Press Foundation
Palestinian Center for Development & Media Freedoms (MADA)
Paradigm Initiative (PIN)
PEN International
Restore the Fourth

Social Media Exchange (SMEX)
SocialTIC
South East Europe Media Organisation (SEEMO)
South East European Network for Professionalization of Media (SEENPM)
Southeast Asia Freedom of Expression Network (SAFEnet)
Statewatch
Surveillance Resistance Lab
Surveillance Technology Oversight Project (STOP)
Syrian Center for Media and Freedom of Expression
TEDIC
The Tor Project
Unwanted Witness
Valerie Steeves, Full Professor, Department of Criminology, University of Ottawa
Vigilance for Democracy and the Civic State
Wolfgang Kleinwaechter, Professor Emeritus, University of Aarhus, former ICANN Board Member