Joint Letter to the European Union and its Member States concerning the United Nations Cybercrime Convention

We, the undersigned organisations and individual experts, urge all EU member states to vote no when the draft UN Convention against Cybercrime (A/AC.291/L.15) comes to a vote at the General Assembly.

We are united in urging the EU and its member states to reject the proposal to adopt the Convention during the UN General Assembly vote. The breadth and depth of opposition to the draft UN Cybercrime Convention is stark – bringing together human rights groups, media freedom organisations, the Office of the UN High Commissioner for Human Rights (OHCHR), leading security researchers, large tech companies, and industry associations – and indicates the need for a clear departure from the current, damaging and misguided, approach. A decision to withdraw support would not prevent the EU and its member states from continuing to engage in the development of human rights compliant international standards to address cybercrime and capacity building for mutual legal assistance (MLA) requests and preventing and combating cybercrime. Rather, it would provide space for critical reflection and consideration of alternatives.

In contrast, EU support for the adoption of the draft UN Cybercrime Convention would contribute to swift and broad ratification, undermining democracy, human rights and the rule of law, endangering a wide range of communities and jeopardising the safety and privacy of Internet users globally. We urge the EU and its member states to withdraw their support from the draft UN Cybercrime Convention and use their mandates to encourage other countries to do the same.

Key concerns:

The UN Cybercrime Convention is excessively broad and introduces significant legal uncertainty. It provides for states to leverage highly intrusive domestic and cross-border surveillance powers for the purpose of a broadly defined list of criminal offences which bear only a minimal nexus to information and communications technology systems and go far beyond the scope of core cyber-dependent crimes. For instance, Article 23 requires the collection of e-evidence on a wide range of crimes, even those that don't involve information and communication systems, which can be easily misused by governments to stifle dissent. Article 35 requires states to cooperate with each other in the collecting, obtaining, preserving and sharing of evidence in electronic form "for any serious crime", that a country chooses to punish with a sentence of four-year or greater, without robust limitations. Additionally, Article 4 expands the scope of criminalization in the Convention to an indefinite list of possible crimes, in conflict with the principle of legality. It also fails to specify whether a qualifying treaty or protocol must be one adopted by the UN General Assembly, or simply one that has been registered in the UN through Article 102 of the UN charter. The latter would include any number of bilateral and multilateral instruments. In addition, the negotiation of a supplementary protocol to the Convention to address additional criminal offences, risks further expanding the offences criminalised without the requisite conditions and safeguards.

It also lacks clarity concerning the liability of online platforms for offences committed by their users, conflicting with the approach taken in the EU Digital Services. Whereas Article 18 of the Cybercrime Convention lacks the requirement of intentional participation in offences established in accordance with the Convention, Article 19 requires intent. This poses the risk that, in some states parties, 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 – in contrast to the approach taken in the EU Digital Services Act – which could incentivise overly broad content moderation efforts by platforms to the detriment of freedom of expression, and disproportionately impact marginalised communities. In addition, Article 18 of the UN Convention is much broader ("for participation") than the equivalent article in the Council of Europe's Budapest Convention on Cybercrime ("committed for the cooperation's benefit") and lacks the clarification provided by paragraph 125 of the Budapest Convention's Explanatory Report.

In addition to its expansive scope, the draft UN Cybercrime Convention lacks enforceable and mandatory human rights safeguards as well as gender mainstreaming to ensure common understanding among state parties and protect against abuse. In particular, the absence of prior authorization, notification where an individual is subject to the Convention's powers, and core human rights principles of legality, necessity and non-discrimination from Article 24 (Conditions and Safeguards) is deeply concerning. The provision is also limited in its application, applying only to powers covered by Chapter IV (Procedural Measures and Law Enforcement) to the extent these are implicated when responding to a request under Chapter V (International Cooperation), rather than to the Convention as a whole. This means, in practice, that much of the cross border evidence sharing under the draft Convention is authorised without any meaningful conditions and safeguards.

Moreover, while acknowledging the importance of gender mainstreaming in the preamble, a gender perspective is only included in Article 34 on the protection of victims and addressed in Article 53(h) on preventive measures which may include fighting gender-based violence. Neither reference aims to mainstream gender throughout each article nor to the treaty as a whole; and civil society's calls to at least include specific references to gender in crucial Articles 24 and 36, for example, were omitted. This omission from the UN Convention reflects the significant opposition to advancing gender equality in the digital age from some governments and is a missed opportunity to ensure that the draft Convention does not undermine human rights on the basis of gender.

Of similar concern are the international cooperation provisions, which risk undermining the level of data protection guaranteed by EU law. Article 40 of the UN Convention requires state parties to provide "the widest measure of mutual legal assistance" and risks conflict with domestic law and EU data protection law in EU member states relating to the transfer of personal data. This article may unduly incentivize the transfer of the personal data subject to appropriate conditions under Article 36(1)(b) (also of the UN Convention), for example through derogations for specific situations in Article 38 of the EU Law Enforcement Directive. Article 36(1)(c) of the UN Convention also encourages States Parties to establish bilateral and multilateral agreements to facilitate the transfer of personal data, creating a further risk of undermining the data protection guarantees of EU law. Additionally, Article 36(2) of the UN Convention fails 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.

Furthermore, the international cooperation provisions of the UN Convention risk facilitating cross-border human rights violations. This poses grave risks to a range of at-risk communities, including those persecuted on the basis of gender, race, sexual identity and other protected characteristics, those critical of their governments, diasporic communities, whistleblowers and others. Endorsing the draft UN Cybercrime Convention paves the way for triangular cooperation requests to EU member states, whereby one non-EU state party (state A) renders cooperation with an EU state party (state B) by transmitting information relating to criminal matters without prior request under Article 40(4) of the UN Convention, thereby triggering the starting of an investigation in the EU member state (state B). Afterwards, the non-EU state party (state A), or even a third country (state C), could start a process requesting cooperation from the EU member state (state B) to access information gathered in this newly opened procedure. While the draft Convention provides grounds for refusing requests that would permit the suppression of human rights, the lack of precise and operative safeguards and deference to domestic criminal law provides considerable scope for abuse.

In addition, a number of provisions in the draft UN Cybercrime Convention establish information-exchange mechanisms that bypass mutual legal assistance (MLA) procedures and the limited safeguards provided. Article 47 authorises direct police cooperation between states parties without any MLA request; the lack of an MLA request as a basis for cooperation not only means that MLA vetting authorities are not involved, but also that many of the international cooperation safeguards – which are premised on the need for a "request" such as Articles 40(21) and 40(22) – do not apply. Article 41 relating to the 24/7 network would require short notice cooperation for activities such as locating a suspect, again in relation to any serious crime. While the EU Law Enforcement Directive would apply to EU member states engaged in direct police exchanges under Article 47, there is no requirement for other police agencies participating in data exchanges to have adequate data protections in place, meaning that Article 47 could be used to exchange sensitive, repurposed evidence between these agencies.

Viewed in its totality, rather than promoting a more secure Information and Communication Technologies environment, the draft UN Cybercrime Convention risks making us less secure. For example, the Convention fails to incorporate language sufficient to protect good-faith actors – such as security researchers, whistleblowers, activists, and journalists – meaning that vital cybersecurity work will be exposed to excessive criminalization due to the absence of a qualified standard of malicious intent or clearly articulated public interest defence. In addition, Article 28(4) – relating to the search and seizure of electronic data – risks being interpreted by governments to compel technology companies' employees to provide the necessary information for the purpose of undermining security safeguards to facilitate surveillance. This could result in a range of abuses: from the employees of technology companies being detained while travelling abroad, to forcing such employees to reveal confidential information – including weaknesses and unpatched vulnerabilities in the employer's product or the handling of encryption keys--, contrary to the instructions of their employer.

The draft UN Cybercrime Convention compounds many of the problems in the Budapest Convention while introducing new ones. It replicates intrusive and problematic powers adopted in the Budapest Convention without adding meaningful safeguards against abuse. The proliferation of commercial spyware, for example, is now recognized as a global threat to human rights. Yet Articles 28, 29 and 30 of the draft UN Cybercrime Convention fail to exclude the collection of stored or intercepted data that was accessed through the use of commercial spyware. Article 40, which provides wide-ranging evidence sharing capabilities, further fails to preclude the sharing of information obtained from devices that were accessed illegally through the use of commercial spyware.

In addition, the draft UN Cybercrime Convention lacks many of the critical safeguards that are housed in the Budapest Convention's explanatory report. For example, the UN Cybercrime Convention's criminal provisions rely heavily on the concept of "without right", a term that the Budapest Convention's explanatory report uses to shield standard tools and protocols (paragraphs 48 and 58), the dissemination of cyber security tools (paragraph 77) as well as encryption and anonymization tools like VPNs (paragraph 62). There is no counterpart definition to the concept of "without right" in the draft UN Cybercrime Convention or in international law, leaving few limits on how states will apply the broadly framed criminal provisions. Notably, under the draft UN Cybercrime Convention, these provisions are subject to broad jurisdictional parameters – a state may assert jurisdiction over any activity that impacts one of its nationals (Article 22(1)(a) – as well as broad obligations to cooperate on investigations and assess extradition requests, subject to narrowly framed grounds of refusal. Collectively, this approach and lack of clarity puts critical activities of security researchers, whistleblowers and others at dire risk.

To avoid potential conflict with existing EU laws, undermining proportionate and rights-respecting efforts to address cybercrime, and producing significant risks to Internet users globally, we urge the EU and its member states to reject the proposal for the UN General Assembly to adopt the draft UN Convention against Cybercrime and to use their mandates to encourage other countries to do the same.

This statement is supported by the following organisations and individual experts:
Access Now
Amnesty International
ApTI, Romania
Asli Telli, WISER at Wits University
Centre for Feminist Foreign Policy (CFFP)
Chaos Computer Club
CyberPeace Institute
Digitalcourage
Douwe Korff, Emeritus Professor of international law, London Metropolitan University
Electronic Frontier Foundation (EFF)
Electronic Frontier Norway
Electronic Privacy Information Center (EPIC)
epicenter.works – for digital rights
European Digital Rights (EDRi)

Fundación Karisma
Global Partners Digital (GPD)
Homo Digitalis
Human Rights Watch
IFEX
International Press Institute (IPI)
IT-POL
Politiscope
Privacy International
R3D: Red en Defensa de los Derechos Digitales
SHARE Foundation
Statewatch
TEDIC
Wikimedia Europe
Wikimedia Foundation