



Negotiation of procedural rules for and draft protocol to the United Nations Convention against Cybercrime

Submission to the European Commission's call for evidence

July 2026



UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

*Representation Office
to the European Union*

European Commission – Call for evidence concerning the negotiations for the rules of procedure of the future Conference of the States Parties and on a draft protocol to the United Nations Convention against Cybercrime

Submission of the Office of the United Nations High Commissioner for Human Rights

29 July 2026

The *Office of the United Nations High Commissioner for Human Rights* (OHCHR/UN Human Rights) is the leading United Nations entity on human rights. OHCHR is mandated to speak out objectively in the face of human rights violations and help elaborate the standards that are used to evaluate human rights progress worldwide. This mandate also includes human rights as they relate to the use of digital technologies. Under the United Nations Global Digital Compact, OHCHR is to provide advisory services to stakeholders to align digital governance and regulation of digital technologies with international human rights norms and standards.

OHCHR welcomes the opportunity to provide comments on the forthcoming negotiations for the *Rules of Procedure* of the future *Conference of the States Parties* and on a draft protocol to the *United Nations Convention against Cybercrime*.

I. Rules of Procedure

The Rules of Procedure, once adopted, will be a significant legal and institutional text. They will shape the modalities of the Conference of the States Parties, including for the review of the Convention's implementation, for making recommendations for improvements, for subsequent work related to the Convention and even for the elaboration of possible future additional protocols. For that reason, the Rules should be designed to promote transparency, inclusivity, accountability and full respect for human rights.

1. Stakeholder participation strengthens the Conference of the States Parties

One of the most important objectives of the Rules of Procedure should be to guarantee strong, meaningful and inclusive participation by a broad range of stakeholders. Article 57(5) of the Convention expressly recognizes the role of “non-governmental organizations, civil society organizations, academic institutions and private sector entities” in the activities of the Conference of the States Parties. The Rules of Procedure should give practical effect to that recognition through clear, predictable and rights-respecting modalities for participation.

As OHCHR has highlighted in its submissions to the *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, meaningful, inclusive participation, including by voices not usually heard in intergovernmental processes, brings diverse perspectives and practical expertise. It gives States Parties a fuller picture of implementation challenges and helps prevent blind spots, especially in an area where technical, criminal justice, cybersecurity, social science and human rights expertise are all directly relevant.

This is particularly important because decisions taken in multilateral settings can have direct effects on national laws, institutional practices and the rights of individuals. The interconnectedness of domestic and international decision-making requires deliberations in the Conference of the States Parties to draw on a broad range of insights and to remain open to those affected by cybercrime policies and by the investigative powers used to combat it.

2. Human rights as a guiding principle of the Conference

Article 6 of the Convention recognizes the strong link between combating cybercrime and respecting, protecting and promoting human rights. The Convention's effective implementation will therefore depend on integrating human rights throughout its application, including in the work of the Conference of the States Parties, its subsidiary bodies and any review or follow-up mechanisms.

Human rights law requires States to respect, protect and fulfil the rights of every individual to freedom of opinion and expression, access to information, peaceful assembly and association, participation in public affairs and protection against unlawful or arbitrary interference, including by non-State actors. These rights apply not only at the domestic level but also to other levels of decision-making, including intergovernmental processes.¹ Accordingly, States should ensure meaningful and inclusive avenues for participation by relevant stakeholders in the activities of the Conference of the States Parties, including in the exchange of information, coordination and cooperation, review of implementation and elaboration of supplementary protocols.

Embedding human rights in the Rules of Procedure would also strengthen the legitimacy and quality of the Conference's work. Participation by stakeholders with relevant expertise can help identify how both cybercrime itself and measures to counter it affect victims, persons in vulnerable situations, journalists, human rights defenders, researchers, lawyers, children, minorities and other groups that may face particular risks online or in criminal justice processes.

¹ United Nations High Commissioner for Human Rights, Procedures and practices in respect of civil society engagement with international and regional organizations, [A/HRC/38/18](#); see United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association, [A/69/365](#).

3. Recommendations for the Rules of Procedure

OHCHR recommends that the Rules of Procedure provide for meaningful stakeholder participation through the following elements:²

- *Continuity of participation.* Given the important contributions made by non-State stakeholders during the negotiations of the Convention, the Rules should ensure at least the level of participation achieved during that process. Stakeholders admitted to the Ad Hoc Committee process should retain observer status in the Conference of the States Parties through a clear “grandfathering” provision.
- *Participation in plenary and subsidiary bodies.* Both the plenary and subsidiary bodies of the Conference should be open to admitted stakeholders. Excluding stakeholders from subsidiary bodies would deprive States Parties of crucial expertise precisely where detailed work on implementation, technical questions, safeguards and future protocols is likely to take place.
- *Inclusive access for different categories of stakeholders.* The Rules should provide access for ECOSOC-accredited and non-ECOSOC-accredited non-governmental organizations, civil society organizations, academic institutions, private sector entities and relevant international organizations. Expertise required should be defined broadly enough to include experts and stakeholders from all relevant fields, such as cybercrime specialists, cybersecurity researchers and practitioners, computer scientists, social scientists, criminal justice experts, data protection experts and human rights experts.
- *Clear, transparent and timely admission procedures.* Admission procedures should be simple, objective and transparent. They should be completed sufficiently early to allow stakeholders to prepare and participate effectively. Information on applications, objections and decisions should be made available in a timely manner. Any objection by a State Party to the participation of a stakeholder should be limited to compelling and objective reasons, communicated in writing and subject to a transparent process. Stakeholders should have a meaningful opportunity to respond to, or seek review of, an objection before a final decision is taken.
- *Robust participation rights.* Admitted stakeholders should have access to all relevant documents, including draft texts and reports; the ability to attend plenary and subsidiary body meetings; speaking rights at appropriate points in the agenda; and the ability to provide written submissions without unnecessary word limits or procedural barriers.

² See also the submission to the Ad Hoc Committee of 23 January 2026, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/RoP_session/Comments_by_stakeholders/OHCHR_23_January_2026.pdf.

- *Transparency of documentation and proceedings.* The Rules should favour public availability of documents, schedules, draft agendas, meeting outcomes and submissions, subject only to narrowly tailored exceptions. Transparent procedures will improve trust in the Conference and facilitate evidence-based implementation.

II. Possible additional protocol

General Assembly resolution 79/243 mandated the Ad Hoc Committee to continue its work “with a view to negotiating a draft protocol supplementary to the Convention”. This mandate is process-oriented rather than outcome-determinative. The phrase “with a view to negotiating” does not predetermine that a protocol must be adopted, nor does it settle the scope, content or legal effect of any future instrument. Those matters remain for negotiation by States.

Having followed and contributed to the negotiation of the Convention, OHCHR recalls its foundational recommendations submitted to the first session of the Ad Hoc Committee in January 2022.³ Throughout the process, OHCHR also made specific recommendations on the scope of criminalization, procedural measures, international cooperation and the safeguards required by international human rights law.⁴

1. Use the protocol negotiations to strengthen safeguards

The protocol negotiations provide an important opportunity to strengthen safeguards applicable to both the protocol and the Convention itself. While the final Convention includes welcome provisions, including article 6, it does not contain sufficiently specific safeguards for many procedural measures and international cooperation mechanisms. The protocol process should be used to close those gaps.

In particular, OHCHR encourages States to consider safeguards that include:

- clear requirements of prior judicial or other independent authorization for intrusive investigative measures;
- precise limitations on the scope, duration and purpose of procedural powers;
- specific transparency and notification requirements, subject only to necessary and proportionate limitations;

³ https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf.

⁴ See https://www.unodc.org/unodc/cybercrime/ad_hoc_committee/home, for example https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/AHC4_OHCHR_comments_10_January_2023.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/OHCHR1.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/OHRC_AHC_Cybercrime_-_reconvened_concluding_session.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_1_OHCHR.pdf.

- protection for privileged and confidential communications, including communications between lawyers and clients, journalists and sources, and other relationships protected under international human rights law;
- dual criminality requirements and strengthened grounds to refuse cooperation where there is a real risk of human rights violations;
- robust data protection standards, including purpose limitation, data security, retention limits and effective remedies; and
- effective oversight, accountability and remedy mechanisms for individuals affected by investigative measures or international cooperation.

Such safeguards would improve the Convention's practical effectiveness by helping ensure that measures taken to combat cybercrime are lawful, trusted and sustainable. They would also help prevent anti-cybercrime measures from being misused to restrict protected expression, target civil society or enable unlawful surveillance.

2. Avoid overbroad or content-based offences

Several States have suggested the possible inclusion of additional criminal offences. However, the mandate of the Ad Hoc Committee does not require adoption of a protocol containing new offences, while the negotiations of the Convention demonstrated strong resistance against a widening of the scope of criminalisation. If additional offences are considered, they must be carefully delineated in full compliance with international human rights law.

Any additional offence should pursue a legitimate objective and be defined clearly, precisely and narrowly. It should meet the requirements of legality, necessity and proportionality and avoid wording that permits overbroad or discriminatory interpretations. Offences should be limited to conduct that is genuinely cyber-dependent or where the use of information and communications technology is essential to the nature of the harm addressed.

OHCHR reiterates its recommendation to avoid the inclusion of content-based offences. Cybercrime laws have been used in some contexts to impose overly broad restrictions on freedom of expression, including by criminalising online content related to extremism, terrorism, public morals, or hate speech in vague or expansive terms. A future protocol should not lend itself to becoming a basis for justifying such human rights violations.

III. Integration into the EU global digital strategy

OHCHR further welcomes this opportunity to contribute as it reflects the EU's broader commitment to integrate human rights through its international digital strategy, and the Team-Europe guide to a human-centric approach to digital cooperation. To this end, it would also be important to consider broader questions on human rights which the Convention brings into sharp relief. Firstly, the phenomenon of transnational repression has now been broadly recognized as a growing challenge. The increase in police cooperation across borders likely to arise from the Convention, should be met with adequate safeguards and resources to deal with cases of transnational repression. Furthermore, as the EU itself reshapes its own laws under its landmark law the General Data Protection Regulation, due consideration should be given to how changes to the definition of personal data could impact international transfers of data in particular.

Conclusion

OHCHR reaffirms its commitment to supporting Member States in combating cybercrime in a manner that advances human rights, the rule of law and accountability. The Rules of Procedure and any future protocol should reinforce, not dilute, the Convention's human rights commitments. Clear participation rights, transparent procedures and strong safeguards will be essential to ensuring that the Convention contributes to effective cybercrime responses while protecting the rights and freedoms of all individuals.

[END]