CyberPeace Institute's Submission

to the Reconvened Concluding Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

The CyberPeace Institute[1] appreciates the opportunity to comment on the revised draft of the UN Cybercrime Convention (A/AC.291/22/Rev.3). This statement builds upon previous submissions made by the CyberPeace Institute at the previous sessions of the Ad Hoc Committee[2,] in particular, the submission in January 2024 and reflects the Institute's expertise and track record in providing support to vulnerable victims of cybercrime.[3]

---

[1] The CyberPeace Institute is an independent and neutral non-governmental organization that strives to reduce the frequency, impact and scale of cyberattacks, to advocate for responsible behavior and respect for laws and norms in cyberspace, and to assist vulnerable communities.

[2] CyberPeace Institute's Submission to the Seventh Session of the Ad Hoc Committee, January 23, 2024, https://cyberpeaceinstitute.org/news/proposed-cybercrime-convention-risks-making-cyberspace-less-secure/

CyberPeace Institute's Submission to the Sixth Session of the Ad Hoc Committee, August 21, 2023, available at: https://cyberpeaceinstitute.org/news/un-cybercrime-convention-submission; CyberPeace Institute's Submission to the fifth Session of the Ad Hoc Committee, April 14, 2023, available at: https://cyberpeaceinstitute.org/news/submission-to-ad-hoc-committee-on-cybercrime; CyberPeace Institute's Submission to the fourth Session of the Ad Hoc Committee, January 18, 2023, available at: https://cyberpeaceinstitute.org/news/statement-un-ad-hoc-committee-cybercrime-2023

[3] The CyberPeace Institute runs several initiatives helping NGOs globally. Under the Humanitarian Cybersecurity Center, the Institute coordinates recovery efforts after cyberattacks and helps NGOs become more cyber resilient. Furthermore, as part of this free cybersecurity support offered by our flagship CyberPeace Builders, the Institute has been able to analyse the impacts of a number of cyber incidents on the humanitarian sector and, importantly, identify and evidence the vulnerability of NGOs. See more details: https://cyberpeaceinstitute.org/humanitarian-cybersecurity-center.

The CyberPeace Institute also participates in the UnderServed project, an EU-funded initiative from the Internal Security Fund (ISF) aiming to address the lack of adequate cybersecurity measures for vulnerable sectors, including humanitarian, development, and peace non-governmental organisations (NGO). See more details:

Since 2021, the CyberPeace Institute has consistently been expressing doubts and criticisms of, as well as recommendations to improve, the proposed UN Cybercrime Convention. The CyberPeace Institute and its partners have been sounding the alarm for three years, including through the 2021 Multistakeholder Manifesto supported by over 50 civil society and industry representatives and Joint Statement "Revisiting the Multistakeholder Manifesto at the 11th Hour" published on 23 January 2024, but to no avail.

The CyberPeace Institute is seriously concerned that States are spending enormous resources on a treaty which will not address the real systemic issues of fighting cybercrime, and will create unacceptable risks to human rights.

General provisions (Chapter I.)

The proposed Convention still remains too broad in scope and contains measures that undermine human rights protection. The CyberPeace Institute reiterates the requirement for a narrow scope for the proposed Convention that focuses solely on cyber-dependent crimes. A narrow scope of application should be taken that is strictly limited to the investigation and prosecution of serious cyber-dependent crimes while preserving the confidentiality, integrity, and availability of digital services and personal data.

A criminal justice instrument that aims to prevent and counter cybercriminal activities must be rooted in the protection and promotion of human rights and cannot work against them.

The CyberPeace Institute wishes to reiterate that the primary purpose of the Cybercrime Convention must be to respond to the needs of cybercrime victims and support the efforts to obtain justice and remedy for those affected by cybercrime. The damage wrought by cybercrime has an important human component. A new international treaty against cybercrime must advance evidence-led accountability. This includes ensuring that the harms affecting, and experiences of, cybercrime victims are fully considered, and the necessary protections and support to victims of cybercrime

---

https://cyberpeaceinstitute.org/news/uniting-to-protect-vulnerable-sectors-from-cybercrime-launch-of-the-eu-funded-underserved-project

are provided. The Convention must consider different types of harm inflicted on people by cybercrime as some individuals and groups may be disproportionately targeted, affected, or otherwise disadvantaged or vulnerable to its impacts, and where the harms and impact on the safety and well-being of people are consequent.

Whilst the CyberPeace Institute is well aware of the threats posed by cybercrime, a Cybercrime Convention will only be effective if it facilitates victim's access to repair and redress, strengthens investigative capacity, and upholds fundamental rights. It must demonstrate a state's ambition to protect its people.

The multistakeholder community has consistently raised alarm that this draft Treaty risks becoming a tool that justifies and facilitates States' violations of human rights. This is not an abstract concern. It is extremely concerning that there is a global rise in the use and misuse of cybercrime instruments and legislation by some governments citing national security concerns, maintaining social order, and fighting terrorism in order to restrict privacy, freedom of expression, assembly and association, and target and surveil individuals and groups. States are urged to ensure that the Convention is not able to be exploited by States with a poor human rights record who seek to justify human rights abuses under the guise of combating cybercrime.

Regarding ***Article 2. Use of Terms***, we believe that references to the broad group of Information and Communications Technologies (ICTs) misused for criminal purposes and similar outdated references are problematic and may support an expansive approach to criminalization resulting in restrictions on a broad range of activities, some of which are not criminal.

The Convention should use the terms "computer system" and "computer data" rather than putting forward new or overbroad terms that can introduce uncertainty into the scope of the defined terms and hinder international cooperation. More than 120 countries already use these terms as defined in the Budapest Convention[4], which has served as a guideline to States globally and facilitated harmonization of legislation around the world. Correspondingly, the term 'cybercrime' is well-established, specific and can achieve consensus as it enjoys broad recognition across the international community.

[4] Jan Kralik, Budapest Convention on Cybercrime: Content, impact, benefits and process of accession. PGA Regional Caribbean Workshop, July 5-6, 2023, available at: https://www.pgaction.org/pdf/2023/2023-07-06-presentation-by-mr-kralik-council-of-europe.pdf

Article 3. Scope of application[5] must be limited to the core cyber-dependent crimes. This article should be tied to the scope of criminal offenses listed in Chapter II (articles 7 to 17) and avoid ambiguity that may facilitate the use of investigative powers and procedures for less serious crimes or crimes that may violate States' human rights obligations. The CyberPeace Institute welcomes the proposal made by Canada[6] for a new Article 3.3 intended to bring further clarity to the scope of the Convention and limit its potential to interfere with broader obligations and responsibilities as UN Member States. Still, safeguards must be mainstreamed throughout the text.

Article 4. Offenses related to other United Nations conventions and protocols must be deleted or detailed and clarified to ensure a narrow scope and clear application of the Convention. The current open-ended scope of this provision makes it impossible to assess its future impacts as it goes far beyond cybercrime.

Article 6. Respect for human rights misses the opportunity to strengthen compliance with human rights standards. The provisions must additionally include references to the principles of legality, necessity, and proportionality together with mechanisms ensuring transparency, oversight, and access to remedies. We recommend adding references to specific instruments in Article 6(1), such as, and non-exhaustively, the International Covenant on Civil and Political Rights (ICCPR, 1966). In addition, other rights particularly affected by the Convention shall be added to the existing list in Article 6(2). We also recommend including specific human rights safeguards across the text to mainstream this general obligation and have safeguards applied and tied to specific provisions. Any disconnect between chapters of this Convention risks creating legal uncertainty that can be exploited to justify laws and practices that do not comply with human rights law and other international human rights obligations.

Criminalization (Chapter II.)

---

[5] The new draft reserves for further discussion in the informal negotiations *most* of the scope articles (articles 3, 35 and 40(2) are all italicized) and the safeguards articles, hence, the approach to these is not yet decided. Still, the proposals by the co-facilitators and discussions within the substantive sessions strongly indicate a widening of the scope and a watering down of the safeguards.

[6] Proposal by Canada on behalf of a group of 39 States and the European Union to the Ad Hoc Committee on Cybercrime (AHC) to further define the scope of the draft Convention, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Canada_proposal_3.3.pdf

This Convention should be limited to cyber-dependent crimes committed by using computer systems and the text should require a standard of criminal intent to ensure that legitimate activities are not criminalized. Any other consensus-based cyber-enabled offenses, which may be part of this Treaty, must be defined narrowly, be consistent with international human rights standards, and be based on consensus. As it stands, this Convention criminalizes legitimate activities such as the work of cybersecurity researchers, ethical hacking, and pen-testers that keep the digital ecosystem secure. These good-faith activities are fundamental to securing the online ecosystem from criminal abuse and must be exempt from the Convention's scope. Creating legal ambiguity for cybersecurity professionals will make online systems more exposed and vulnerable to cybercrime, and work against the Convention's stated purpose. To avoid this, the Convention should include language that exempts individuals engaged in lawful cybersecurity practices, and as a minimum ensure that the element of "criminal intent" is included as a common requirement. An alternative could be to introduce the elements of "criminal intent" and harm as mandatory by replacing "may" with "shall" in relevant articles. Generally, we recommend avoiding references to ambiguous standards such as 'dishonest intent', 'without authorization' or 'without right'.

Jurisdiction (Chapter III.)

To enhance global efforts against cybercrime, this Convention must prevent conflicting demands, harmonise rules across jurisdictions, and prevent frictions with existing international obligations and instruments. The text needs to provide clear guidance on which jurisdiction applies in investigating and prosecuting criminal offences covered by this Treaty. States must avoid adopting an instrument that could inadvertently give rise to jurisdictional disputes and create obstacles to effective international cooperation. Neither States nor private actors can effectively cooperate if they face conflicting demands. The Convention should also not allow for expansive claims of extraterritorial jurisdiction. States should avoid language that can create conflicting obligations for service providers or data custodians, who may be forced to violate law in one jurisdiction to comply with a data request in another.

Procedural Measures and Law Enforcement (Chapter IV.)

The proposed scope for procedural and law enforcement powers expands state surveillance and applies to the collection of electronic evidence related to virtually any crime, including non-cybercrime offenses. Widening the scope of this Chapter to cover all crimes committed with the use of an ICT significantly risks undermining human rights, including the right to privacy and the right to a fair trial. ***Article 23. Scope of procedural measures*** should be constrained to the offences included in the criminalization chapter, articles 7-17, to avoid uncertainty and prevent any potential harm.

The current wording of ***Article 24. Conditions and safeguards*** are insufficient and should be strengthened according to the principles outlined above. Conditions and safeguards must be consistently applied throughout the international cooperation chapter. The Convention must define government access to personal data narrowly and precisely to protect human rights and fundamental freedoms, including the privacy of personal data, and guarantee the right to redress. Its provisions must follow the principles of proportionality, necessity, and legality and be accompanied by mechanisms safeguarding human rights to prevent potential misuse.

Article 28. Search and seizure of stored computer data is highly concerning. As it stands now, it can result in State Parties imposing legal obligations upon third parties, such as a service provider or data custodian, to disclose vulnerabilities or provide relevant authorities with access to encrypted communications. Such provisions infringe on the right to privacy, interfere with cybersecurity measures, pose a threat to the security, integrity, and confidentiality of online communication channels and could undermine trust in secure communications. States Parties to the Convention must avoid endorsing any surveillance powers that can be abused to undermine cybersecurity and encryption. We recommend the deletion of Article 28(4).

The practice of real-time collection of traffic data has been determined by many States as an invasion of privacy and fundamental freedoms and as a violation of the principles of necessity and proportionality of data collection. Therefore, intrusive powers for real-time collection that can facilitate domestic spying should be deleted from the Treaty. We recommend the deletion of ***Articles 29. Real-time collection of traffic data*** and ***Article 30. Interception of content data*.**

There are remaining substantial gaps among States in the level of personal data collection and protection, including concerns about the rule of law and the lack of

impartiality and independence of the judiciary in some countries. Overall, the provisions under this chapter and across this Convention should be not only in line with domestic law but consistent with obligations under international human rights law to prevent this criminal justice instrument from being implemented in ways that can violate human rights. This is particularly problematic when States' existing domestic laws and practices are inconsistent with international human rights law, as is too often the case.

The main purpose of a new international law against cybercrime should be to protect victims, witnesses and others whose lives have been impacted and harmed by cybercrime. Effective remedies, assistance, and redress mechanisms must be available to these individuals or groups. From the outset, the CyberPeace Institute has called for the prioritizing of victim protection and improving their access to justice. Unfortunately, the current draft offers weak support for those impacted by cybercrime, making the needed assistance and protection only optional and deferring to domestic law that may or may not offer adequate protection, remedies, and redress mechanisms. This leaves victims with no legal guarantees or rights to seek recourse and return of property. The fight against cybercrime must consider the significant human impact and harm, often on the most vulnerable in our communities. The text should be revised to require robust protections for victims and witnesses of cybercrime outlined in ***Article 33. Protection of witnesses*** and ***Article 34. Assistance to and protection of victims*** in line with international standards and human rights law.

International Cooperation (Chapter V.)

As stated above, this cybercrime treaty must have a narrow and clearly defined scope limited to the crimes listed in Chapter II of this Convention that guides the areas of international cooperation. Otherwise, intrusive digital surveillance and data access powers could extend to a vast array of other activities considered criminal that use technology. Disappointingly, the revised text expands the coercive powers of governments to investigate, detain, and prosecute individuals and presents significant risks, especially to people in positions of vulnerability.

Article 35. General principles of international cooperation should have a narrow scope to facilitate international cooperation for the purpose of investigating and prosecuting criminal offenses set out in *Articles 7 to 17* as cooperation beyond those Convention offenses becomes potentially problematic. We recommend Article 35(1) be narrowed

to provide for international cooperation for the purpose of investigating and prosecuting the crimes recognized under Chapter II.

International cooperation on cybercrime must require high standards for data protection, in particular in ***Article 36. Protection of personal data*** and related provisions. A lack of safeguards, transparency, and due process when accessing personal data can facilitate intrusive digital surveillance and data access powers. Provisions guiding the cooperation between States should not defer extensively to domestic laws but ensure that respective bodies are handling personal data in accordance with established international principles to guarantee fairness, transparency, accountability, and effective oversight over handling personal data. Due diligence requirements, including lawful and fair processing, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality should be observed by all State Parties. We recommend that Article 36 be amended to reflect international data protection principles derived from existing international human rights law.

Technical Assistance and Information Exchange (Chapter VII.)

Technical assistance requires serious considerations regarding its human rights impact and potential unintended consequences as it poses risks of eventuating into inadvertent harm. This is doubly true in cases of States or private companies providing access to dual-use technologies that may eventuate into the abuse of surveillance technologies such as spyware. We recommend **Article *54. Technical assistance and capacity-building*** is conditional and subject to a human rights and impact assessment that informs and guides all such activities, the scope, consequences, and the exchanged and employed tools before such activities are undertaken, adheres to international human rights law, and is subject to independent oversight. Finally, capacity building in the cyber domain does not happen in a vacuum and other UN venues can provide important guidelines that have been already agreed upon by consensus.

Absent the important changes required, we call on delegations to reject the draft Treaty and not advance it to the UN General Assembly for adoption.