CyberPeace Institute's Submission

to the 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.1). Our recommendations aim to strengthen the text of the Convention and provide human-centric considerations for States engaged in cybercrime negotiations. This statement builds upon the submissions made by the CyberPeace Institute at the previous sessions of the Ad Hoc Committee[2] and reflects the Institute's expertise and track record in providing support to vulnerable victims of cybercrime.[3]

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.[4] Mainstreaming gender across the Convention is important in efforts to prevent and combat cybercrime[5], as such crimes can have differentiated impacts and severity of harms determined by gender identity or expression.[6] A new international law 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 are provided.

The current revised negotiating text causes grave concerns and does not reflect on the principles advocated by the multistakeholder community or the inputs provided over the course of the negotiations. To instructively convey our concerns, the CyberPeace Institute and the Cybersecurity Tech Accord came together to call on States to prioritise human-centric principles in the Convention. Our joint statement **"Revisiting the Multistakeholder Manifesto at the 11th Hour"**[7] leverages the 2021 Multistakeholder Manifesto[8] supported by over 50 civil society and industry representatives as a guide to assess how these principles have been reflected in the UN deliberations.

General provisions (Chapter I.)

The CyberPeace Institute recommends narrowing the scope of the Convention to cyber-dependent crimes specifically defined and included in its text, and for safeguards and international human rights standards to be mainstreamed across the Convention as a whole and throughout each article. In a similar vein, 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 multistakeholder community has consistently raised alarm that this Treaty risks becoming a tool that justifies and facilitates States' violations of human rights. This is not an abstract concern. It is well-documented[9] and extremely concerning that there is a global rise in the use and misuse of cybercrime instruments and legislation by some governments to restrict privacy, freedom of expression, assembly and association, and target and surveil individuals and groups citing national security concerns, maintaining social order, and fighting terrorism. 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.

To accommodate the rapidly evolving nature of cybercrime, the text of a treaty must adopt terms that are technology-agnostic, flexible enough to be future-proof, and specific enough to ease the implementation process. This is especially important in the context of a criminal justice instrument in order to ensure that States' powers and obligations are clear and precise.

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 by invertedly 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[10], 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.

Article 3. Scope of application[11] must be limited to the core cyber-dependent crimes. This article should be tied to the scope of criminal offenses listed in Chapter II. 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[12] 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 and the Treaty’s application must be limited to a clearly defined list of core cyber-dependent offences to prevent misuse.

Article 5. 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 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.)

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 offences, 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 now, the draft text encompasses broad and unclear types of conduct outside of the core offences, including cyber-enabled offences and content-related crimes.

The danger that this Treaty can lead to criminalizing legitimate activities and expression, especially for excessively targeted groups such as human rights defenders, journalists, whistleblowers, and political opposition is imminent. The current language also fails to protect legitimate activities of ethical hackers, cybersecurity researchers, 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. We recommend that standards of criminal conduct require criminal intent and harm. Standards such as 'without authorization' or 'without right' risk allowing the criminalization of acts carried out with beneficial intent and increase the likelihood of punishing individuals for behaviour that did not, or could not have been expected to, cause any harm or damage.

The cybercrime negotiations have seen a continuous push by some States to further expand the list of criminalized offenses under this chapter with the aim to increase ambiguity as to the Treaty's scope and application and shape the document into a general data-access treaty. ***Article 17. Offences relating to other international treaties***[13] introduces broad catch-all provisions and can be seen as a backdoor to a narrow scope in the criminalization chapter. It creates legal uncertainty through an open-ended reference to offences covered by other international conventions and protocols. The Convention should not cover ordinary crimes that merely incidentally involve or benefit from the use of computer systems without targeting or harming those systems.

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 offences. 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 to avoid uncertainty and prevent any potential harm.

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. 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.

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.

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 in ***Articles 29. Real-time collection of traffic data*** and ***Article 30. Interception of content data*** should be deleted from the Treaty unless coupled with significant safeguards. Such standards should comprise prior judicial authorization, specificity, time limits, proportionality, transparency, oversight, and effective redress.

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 prioritising 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.)

A 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 6 to 16*** as cooperation beyond those Convention offences becomes potentially problematic. Extending cooperation to any current or future serious crime could enable or obligate international cooperation and mutual legal assistance for any conduct punishable by a maximum imprisonment of at least four years under domestic law when a computer system is involved. Such parameters create legal ambiguity as governments can decide what crimes they consider serious and therefore extend the scope of the Convention's application.

The principle of dual criminality in ***Article 35*** should be made obligatory and not optional. This principle holds that an act is not extraditable unless it constitutes a crime in both the requesting and requested countries. It provides a layer of protection for individuals, as it reduces the chance of States being able to request cooperation for offences that are not universally recognized as criminal and helps to ensure that extradition is not used as a tool for political repression, persecution of people, and other human rights violations. Requests for international cooperation

should be invalid if the principle of dual criminality is not fulfilled and the relevant provisions should be further secured with references to the necessity of these requests meeting international safeguards and standards protecting human rights.

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.

Provisions guiding global efforts on tackling transnational cybercrime must mainstream the principles of legality, necessity, and proportionality. This chapter should include references to the rule of law, existing international obligations, and international human rights obligations. In the same vein, applicable human rights instruments need to be added to ensure that international cooperation on cybercrime is not infringing on or violating human rights. Articles that are in violation of these principles, such as ***Article 45. Mutual legal assistance in the real-time collection of traffic data*** and ***Article 46. Mutual legal assistance in the interception of content data*** should be removed as they provide intrusive surveillance powers and would allow foreign governments to make requests without mandating equally extensive robust safeguards.

Preventive Measures (Chapter VI.)

The CyberPeace Institute recognizes the importance of preventive measures in fighting cybercrime, including cybersecurity education, capacity building, and awareness raising, and is running a number of projects that support this aim. Non-governmental stakeholders already play an important role in raising awareness regarding the prevention of the offences foreseen to be covered by this Convention.

Article 53. Preventive measures should primarily focus on addressing cybercrime, including protective mechanisms aimed at victims and witnesses, and advancing accountability by prosecuting cybercriminals. The scope of this chapter should avoid duplicating efforts and not be expanded to include cybersecurity measures or increasing the overall societal resilience in cyberspace that are more suitably addressed and developed in other UN, regional, and multistakeholder fora.

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[14]. 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.[15]

Mechanism of Implementation (Chapter VIII.)

Effective implementation of the Treaty must be anchored in an actionable mechanism that puts the Convention into practice while leveraging the strengths of diverse groups of stakeholders. A Conference of the States Parties to the Convention is broadly supported by Member States, however, it needs to be designed as a transparent, informed, and actionable body to serve its purpose of monitoring progress in the implementation and ensure effective oversight.

A clear set of principles on stakeholder participation is needed to guarantee the mechanism's inclusivity, benefit from their expertise and perspectives, and ensure protection for those impacted by cybercrime. For example, organizations that work in proximity with cybercrime victims are vital for sensitising the discussions by

informing them about the lived realities of those affected by cybercrime. Many civil society organizations also provide knowledge of how cybercrime legislation and anti-cybercrime measures impact human rights and different groups of people and build data-driven and experience-based understanding coming from tracking malicious actors and the harm they cause.

Considering the important roles of civil society organizations, industry, academia, and technical experts, their systematic and substantive engagement must be guaranteed in the mechanism of implementation and ***Article 57. Conference of the States Parties to the Convention*** should follow the consensus language on the participation of stakeholders in the work of the Ad Hoc Committee[16].

The Ad Hoc Committee presents a positive example of stakeholder inclusion in UN processes on cyber-related issues. However, the formal openness of cybercrime negotiations did not translate into stakeholders' input and views being integrated in the draft. **The prospect of the current draft being adopted is deeply concerning. Without significant changes, this Convention will facilitate, rather than reduce, cybercrime globally.** We call on States to fully consider the provided feedback and recommendations put forward by the multistakeholder community toward a human-rights respecting treaty that allows for the investigation and prosecution of cybercrime more effectively.

---

[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 behaviour and respect for laws and norms in cyberspace, and to assist vulnerable communities.

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

[4] The damage wrought by cybercrime has an important human component. 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, such as those impacted by cyber incidents targeting essential services and infrastructure. For example, when a cyberattack or incident targets healthcare services or humanitarian NGOs, the harms and impact on the safety and well-being of people are consequent.

[5] Women and girls are particularly vulnerable to cybercrime, especially when those criminal offences are committed by partners or family members as a form of surveillance, control, and continuation of family or intimate partner abuse. See more details: Chatham House, "What Does it Mean to Gender Mainstream the Proposed Cybercrime Convention?" available at: https://chathamhouse.soutron.net/Portal/Public/en-GB/DownloadImageFile.ashx?objectId=5344&ownerType=0&ownerId=191233

[6] Gender can be a factor of vulnerability given the sensitivity of data or other context-dependent repercussions. See more details: Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security," April 2020, Women's International League for Peace and Freedom and the Association for Progressive Communications, available at: https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf

[7] CyberPeace Institute & Cybersecurity Tech Accord, Revisiting the Multistakeholder Manifesto at the 11th Hour, January 16, 2024, available at: https://cyberpeaceinstitute.org/multistakeholder-manifesto

[8] Multistakeholder Manifesto: Prioritizing Human-Centric Equities within the Proposed UN Cybercrime Treaty, September 30, 2021, available at: https://cyberpeaceinstitute.org/multistakeholder-manifesto

[9]Freedom House, Internet Freedom Status 2023, available at: https://freedomhouse.org/explore-the-map?type=fiw&year=2023

[10] 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

[11] The new draft reserves for further discussion in the informal negotiations *most* of the scope articles (articles 3, 35 and 40(2) are all italicised) 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.

[12] 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

[13] Article 17 has been retained for now as informal discussions on the list of offences continue. Its incorporation in the Treaty is still being negotiated. Two key proposals being considered suggest (1.) morph it into a general crimes convention or, potentially, (2.) apply it to the full array of procedural powers and international cooperation. Both options support expansive criminalization, and must be avoided.

[14] European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware calls on the Commission and the EEAS *"to implement more rigorous control mechanisms to ensure that Union development aid, including the donation of surveillance technology and training in the deployment of surveillance software, does not fund or facilitate tools and activities that could impinge on the principles of democracy, good governance, the rule of law and respect for human rights..."* available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html

[15] The UN Open-Ended Working Group on cybersecurity has agreed on a list of widely accepted principles (as agreed in the 2021 OEWG Final Report, A/75/816, paragraph 56) that should be guiding States in capacity building. These principles are based on several considerations such as the process and purpose of capacity building, partnerships, and considerations for people. This last category includes the recognition of the need to respect human rights and fundamental freedoms, consider gender-sensitive, inclusive, and non-discriminatory approaches to capacity building and ensure the confidentiality of sensitive information.

[16] UN General Assembly resolution (A/RES/75/282), available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement