CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

CyberPeace Institute's Submission

to the Sixth 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] welcomes the openness and inclusiveness of this process and appreciates the opportunity to provide recommendations on the proposed draft text of the Convention[2]. These observations aim to contribute to the development of a framework that can serve as a practical tool for international cooperation in preventing, investigating, and prosecuting cybercrime.

The Ad Hoc Committee has engaged in elaborating a future Cybercrime Convention amid a rapid change in the frequency, scale, and sophistication of cybercrime and a growing impact on its victims. The objective of this treaty must be to create avenues for improved access to justice, especially as cybercrime often impacts vulnerable communities and organizations, such as NGOs with scarce resources.

The CyberPeace Institute has been working closely with the most vulnerable victims of cybercrime. Under its Humanitarian Cybersecurity Center[3], and the flagship CyberPeace Builders program for NGOs[4], the Institute coordinates recovery efforts after cyberattacks and helps them become more cyber resilient. By identifying the vulnerabilities that attackers exploit and alerting NGOs to risks and vulnerabilities, the program helps to prevent future attacks on these organizations. Furthermore, as part of this free cybersecurity support, 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.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

Cyberattacks against critical services and organizations affect vulnerable people both physically and online. To effectively protect cybercrime victims, the proposed Convention must recognise their diverse experiences and help in efforts to obtain justice for them. The main purpose of a new international treaty on cybercrime must be to protect and bring remedy to its victims, allowing those affected by cybercrime to seek redress and introducing measures to prevent their re-victimisation.

The Convention should consider different kinds of harm inflicted by cyber incidents on people who are disproportionately targeted or affected in cyberspace. This is particularly important in cases affecting vulnerable groups, or people in vulnerable situations, such as those impacted by cyberattacks targeting the healthcare sector, and other critical infrastructure such as energy, water, and transportation, as well as humanitarian and development organizations.

Mainstreaming gender across the Convention is key to ensuring that this emerging instrument responds to the needs of cybercrime victims. The online domain is an extension of the offline world and can reinforce its abusive structures and multiple biases. Of the estimated 2.7 billion people currently unconnected, the majority deprived of Internet access and use are women and girls.[5] Consequently, they have fewer options to gain digital literacy and this digital divide is a source of further vulnerability to cybercrime. Men have been found to be more likely to commit cybercrimes, including those associated with gender-based offences, such as the use of spyware against partners[6]. At the same time, women and girls are particularly vulnerable to these crimes, especially when being committed by partners or family members as a form of surveillance, control, and continuation of family or intimate partner abuse.

Indiscriminate cybercrime that is not targeting selected individuals or groups can also have differentiated and severe impacts because of gender identity or

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

expression. **Gender can be a factor of vulnerability given the sensitivity of data or other context-dependent repercussions.** For example, when hacked and leaked data includes personal medical information relating to sexual or reproductive history, these leaks can threaten women and LGBTQ+ communities as such information can be used against individuals.[7]

Conclusively, **the future outcome of this Convention will depend on its success in bringing evidence-led accountability and facilitating a remedy for those affected by cybercrime**. States need to reduce the operating space for criminals and hold those responsible for harm accountable through an international instrument that considers the impact of cybercrime on society as a whole as well as its members.

Preamble

The preamble outlines the purpose of the Convention which is anchored in the protection of cybercrime victims. The CyberPeace Institute welcomes the references to the developments in cybercriminal activities and their adverse impact on the well-being of individuals and society (para. 2), the importance of obtaining justice for victims of cybercrime and the necessity to address the needs of persons in vulnerable situations (para. 7), as well as the need for cooperation between States and relevant non-governmental stakeholders in combating cybercrime (para. 9). We also appreciate the affirmation of the importance of mainstreaming a gender perspective in preventing and combating the offences covered by this Convention (para. 10).

The Institute further recommends that the preamble reintroduced the commitment to promoting an open, secure, stable, accessible and peaceful cyberspace for all, where the application of international law and fundamental freedoms are promoted and human rights are protected. **We also recommend further consideration of different kinds of harm inflicted by cybercrime** by

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

stressing the impacts on people who are disproportionately targeted or affected in cyberspace and the differentiated impacts of cybercrime they may experience.

While the preamble is not directly enforceable, it plays a crucial role in determining the context for interpreting the Convention and clarifying the intent of the treaty. Therefore, paragraph 3 is a cause for serious concern. The reference to *"a considerable impact of the use of a computer system on the scale, speed, and scope of criminal offences relating to terrorism, trafficking in persons, smuggling of migrants, illicit manufacturing, or trafficking in firearms, their parts, components, and ammunition, drug trafficking and trafficking in cultural property"* goes far beyond the scope of offences currently proposed in the draft document. **To avoid opening the treaty for wider interpretations, explicit references to a broad scope of existing challenges should be deleted.** Alternatively, this paragraph could adopt the language consistent with other parts of the treaty and be strictly limited to criminal offences covered by this Convention.

Countries must reduce the operating space for cybercriminals. The recognition that States are *"determined to deny safe havens to those who engage in cybercrime by prosecuting these crimes wherever they occur"* (para. 5) stipulates a vital principle for effectively addressing the challenges of transnational cybercrime. These efforts depend on preventing the existence of safe havens that are exploited to evade accountability.

The preamble has seen some improvements since the earlier draft[8] concerning which we stressed the peril of positioning national security against human rights. However, the human-rights language in paragraph 11 could be further strengthened by keeping the focus strictly on respect for human rights and fundamental freedoms. The preceding mention of the need to achieve law enforcement objectives can be removed as this goal is already implied in a criminal justice instrument.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

A rights-respecting and rights-protecting treaty must understand security and human rights as mutually supportive concepts. This approach is consequential because some governments have long exploited cybercrime measures to expand control, broaden surveillance powers, restrict or criminalise free speech, and infringe on privacy. Therefore, we welcome that the preamble acknowledges the right to protection against unlawful interference with privacy including personal data (para. 12).

General Provisions

The scope of the Convention must be clearly defined to avoid unintended implications or consequences and prevent further victimisation and harm. The Institute supports a narrow scope of application 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. To support this goal, this treaty should include strong human rights safeguards, robust independent oversight, and effective redress mechanisms.

A criminal justice system that prevents and counters cybercriminal activities and closes the accountability gap must be rooted in the protection and promotion of human rights and cannot work against them. The respect for human rights as defined in Article 5 is important but should be further strengthened by referencing specific international legal instruments and relevant standards. This extends to the principles of legality, legitimacy, necessity, and proportionality, which are established core principles of international human rights law. Such references will reinforce their applicability in the document and extend the protections they offer in the implementation.

Cybercrime is rapidly evolving in terms of tools and practices and the definitions must follow suit. **A future-proof Convention must adopt terms that are similarly**

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

understood across jurisdictions and that can achieve consensus among countries and streamline the implementation process. Determining the use of terms in a legally binding instrument requires careful consideration of the context in which it will be implemented.

The reference to *"the use of ICTs for criminal purposes"* is problematic. It supports an expansive approach to criminalization that can imply a broad scope of activities in which an ICT device has been used to be considered under the treaty. This is especially dangerous amid an alarming rise in the abuse of legal instruments by repressive governments to criminalise free speech and broaden intrusive surveillance powers targeting civil society representatives, human rights defenders, activists, and journalists. In comparison, **the term 'cybercrime' is narrower and allows for defining the scope of criminalization and international cooperation obligations in a clear and precise way that can support the effective implementation**.

Criminalization

Any future legal instrument should ensure that definitions qualifying behaviour as criminal are constructed with a narrow scope to prevent criminalization of behaviour that constitutes the exercise of fundamental freedoms and human rights. By contrast, a broad scope, especially when coupled with a vague and expanded criminalization chapter, will introduce confusion, delay requests for cooperation, and undermine human rights and fundamental freedoms in the process. Moreover, it could threaten human rights globally by legitimising intrusive investigations and unhindered law enforcement access to personal information that can further harm individuals or groups, especially those that are already disproportionately targeted or impacted in the digital domain.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

The Convention should be limited to cyber-dependent crimes which require computer systems in order to be committed. It should also require a standard of clear criminal intent to ensure that legitimate activities are not threatened by criminalization due to misinterpretation of the provisions and be limited to serious crimes. **A broad scope of criminalization increases the likelihood of duplication and contradiction with existing frameworks and endangers the exercise of human rights online.** This is particularly the case with criminalising content-related offences under this framework, which could lead to violating freedom of speech globally.

The Institute welcomes the relatively narrow approach to criminalization presented in the draft text. We further offer some considerations to ensure that the proposed treaty is fit for the purpose and confined in its scope. The zero draft has introduced a new Article 17 that compels States to apply the Convention to crimes *"established in accordance with other international conventions and protocols."* This provision can imply the implementation of additional cyber-enabled offences, while at the same time, these are not subject to the same standards as offences established in accordance with Articles 6 through 16. This language is overbroad and could be used as a loophole to reintroduce some of the previously excluded crimes.

The Cybercrime Convention should not be shaped into a general crime convention, and crimes with a digital component but not dependent on the use of computer systems should be addressed within their own respective frameworks that are more suitable for this purpose. We recommend removing Article 17 to avoid misinterpretations regarding the applicable international conventions and protocols captured by this provision.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

Procedural Measures and Law Enforcement

The Institute has repeatedly called on States to include robust safeguards throughout the Convention to protect individuals and communities from potential abuse of government powers and law enforcement practices. In line with this condition, **we urge States to limit the scope of application of all procedural measures to clearly defined scope of crimes put forward in the Convention**. The scope of application of procedural measures in Article 23 should be limited to the offenses included in the criminalization chapter to avoid uncertainty and prevent any potential harm. We propose to delete section 2(b) in this article and limit the application of section 2(c) to offences covered by this Convention.

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 is insufficient to achieve this goal. At a minimum, the draft Convention should retain the principles outlined in Article 15 of the Budapest Convention[9] and ideally further extend it to incorporate additional safeguards.

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 of traffic data (art. 29) and interception of content data (art. 30) under investigative provisions should be deleted from the treaty.

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

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

of impartiality and independence of the judiciary in some countries. For this reason, as an overarching principle, the provisions under this chapter and across this Convention as a whole 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.

International Cooperation

A cybercrime treaty must have a narrow and clearly defined scope that guides the areas of cooperation between States. This is a necessary precondition for providing transparent, coherent, and—ultimately—effective international cooperation on cybercrime. Considering that many countries have engaged in this process precisely for the reason to extend and strengthen their cooperation with other countries and regions, **streamlined provisions and widely accepted terms in this chapter are necessary requirements for having this instrument implemented in practice**. Ideally, the Convention will enable collaboration for countries that do not have other means of cooperation on cybercrime and encourage international cooperation between law enforcement and prosecutors. At the same time, it must prevent potential misuse of the provisions as an avenue for States to reduce their existing obligations under international law, especially international human rights law.

The Convention must set high standards for the protection of personal data with robust safeguards for data protection. This is not only an important requirement from the angle of human rights protection but also for facilitating the cooperation that States are seeking to gain from this treaty. **Neither States nor private actors can effectively cooperate if they face conflicting demands.** Countries will not be able to transmit personal data to other jurisdictions if their standards for data protection are not fulfilled. To enhance global efforts against cybercrime, **this Convention must prevent conflicting demands, harmonise rules across jurisdictions, and ensure**

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

synergies with existing international obligations and instruments. As a general condition, international cooperation provisions should not defer extensively to domestic laws. Instead, **this treaty must ensure that States are handling personal data in accordance with established international principles**.

The principle of dual criminality, which holds that an act is not extraditable unless it constitutes a crime in both the requesting and requested countries, is a prerequisite for rights-respecting international cooperation. This condition is necessary to ensure that extradition is not used as a tool for political repression, persecution of people, and other human rights violations. For this reason, **requests for international cooperation should be invalid if the principle of dual criminality is not fulfilled**. The conduct in the draft treaty is limited to serious crimes and Article 35 should not be extended to a wide scope of elusive offences covered by Article 17. References to other crimes beyond this Convention should be deleted.

The safeguards accompanying international cooperation on cybercrime, including grounds for its refusal, must be robust in order to protect individuals and groups that can be vulnerable to the misuse of these provisions. This chapter should incorporate more substantive safeguards and references to international instruments and standards that guarantee transparency and protection persons and their data. Furthermore, it should detail substantial grounds under which a state authority may deny a request for extradition in instances where individuals may be persecuted on account of their race, religion, gender, or other internationally protected personal characteristics.

Preventive Measures

A multi-stakeholder approach is essential for efficient and effective prevention of cybercrime. **Civil society and human rights organizations as well as private actors already lead initiatives that improve the resilience of societies against**

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

cybercrime. This chapter should avoid duplicating efforts focused on wider cybersecurity issues that are more suitably addressed in other fora. Relevant to this treaty, non-governmental stakeholders can play an important role in raising awareness regarding the existence, causes, and gravity of the threat posed by the offences covered by this document and its redress and accountability mechanisms. **Non-governmental organizations contribute to a rule of law ecosystem, provide human rights expertise, and support redress for victims of cybercrime.** Governments can benefit from their experience that is informed by the organizations' proximity to victims. They help to sensitise the oftentimes overly technical discussions by informing about the impacts of agreed measures on people – their well-being, rights, and security.

Non-governmental stakeholders are well-positioned to inform the public about the considerations for individuals and communities stemming from the Convention, especially those in positions of vulnerability. They can also guide initiatives that prevent the treaty's misuse against legitimate activities such as those of ethical hackers and cybersecurity researchers. To fit its purpose, this chapter should highlight the applicability of international human rights law on top of fundamental principles of domestic law. **The most effective preventive tool will be if this Convention focuses on streamlining international cooperation of clearly defined and narrow scope of serious cyber-dependent crimes with clear criminal intent to avoid any abuse or unintended consequences.**

Technical Assistance and Information Exchange

Technical assistance and capacity building are vital for levelling the field for States across diverse regions, and especially for supporting the efforts of developing countries to implement this Convention. However, this chapter also brings important human rights considerations in regard to its wider impact and consequences. Additionally, **capacity building does not happen in a vacuum** and

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

other bodies and venues may be better suited to address the broader cybersecurity needs of countries.

The UN Open-Ended Working Group on cybersecurity has agreed on a list of widely accepted principles[10] 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.

While technical assistance set forth in this Convention centres around fighting cybercrime many general principles can be applied here. For example, the basic common ground for partnerships. To avoid reinforcing negative dynamics between countries and regions through conditional agreements such as existing global inequalities, **technical assistance set in the Convention should be on a voluntary and not mandated basis, needs-driven and without conditions**. We further recommend that it considers the capacity building work done in other relevant areas, and in cooperation with various stakeholders, to meaningfully contribute to effective international cooperation against cybercrime.

Technical assistance in the field of cybercrime poses certain risks that can eventuate into inadvertent harm, especially if it includes providing access to technologies that can be misused such as dual-use tools. For that reason, we recommend that technical assistance is not only permitted under domestic law (art. 54 (3)) but also provided in accordance with international human rights law. It must also be subject to a human rights and impact assessment that informs and guides all capacity building activities, their tools, and the scope before such activities are undertaken.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

Mechanism of Implementation

An effective implementation must have an actionable mechanism that puts the Convention into practice and benefits the victims of cybercrime. The Institute welcomes the establishment of a Conference of the States Parties to the Convention that would be facilitated under UNODC. This kind of periodic review of the Convention's impact and implementation has been broadly supported by Member States as a preferred option and provides a good base to support the long-term effectiveness of the treaty.

However, the Conference could be designed to be more accurate, informed, and sustainable through the deliberate inclusion of the expertise and perspectives of organizations that work in proximity with cybercrime victims such as human rights organizations, civil society, and other relevant organizations. **The impact of cybercrime on society as a whole and its individual members who are disproportionately affected by cybercrime should be considered when holding those responsible for harm accountable.**

The Institute supports the references to cooperation with relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions, and the private sector in Article 57 (1c). Yet, considering the important role that the non-governmental and private sectors have established in this area, their meaningful engagement should be reiterated in the mechanism of implementation.

We encourage putting forward a clear set of principles extending the current wording in Article 57 (6) that outlines receiving inputs from relevant multi-stakeholders. This can be achieved by supporting inclusive and transparent language on stakeholder participation in the envisioned mechanism of implementation. Guidance can be found in the consensus language on the participation of stakeholders in the work of

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

the Ad Hoc Committee, which has been adopted in the UN General Assembly resolution (A/RES/75/282)[11].

Final provisions

As a criminal justice treaty with potentially far-reaching consequences, **this Convention must prevent any instances of possible violations of its provisions against legitimate activities**. Article 59 (1) under final provisions could be strengthened with an additional reference to international human rights law to stipulate that each state will take the necessary measures in accordance with fundamental principles of its domestic law as well as international human rights standards to ensure the implementation of its obligations under this Convention.

In the same vein, such addition is also needed in Article 59 (2), which proposes that States *"may adopt more strict or severe measures than those provided for by this Convention for preventing and combating the offences covered by this Convention."* Human rights safeguards clearly referenced here and throughout the document are necessary to ensure that the treaty does not become a tool for restrictions that would violate human rights and fundamental freedoms.

Finally, we would like to reiterate that **the focus of the proposed Cybercrime Convention should be on protecting targets of cybercrime and offering adequate remedies and redress to the victims**. This objective must be reflected in the narrow scope of criminalization, robust human rights safeguards, clearly defined terminology that supports the narrow scope for interpretation, principle-based capacity building and an active involvement of relevant non-governmental actors in the drafting and implementation process.

Countering cybercrime requires a whole society approach. A multi-stakeholder approach is vital to address the challenges of transnational cybercrime in an

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

effective, impactful, and sustainable manner. Our collective goal is to ensure that human rights and fundamental freedoms are respected and prioritised in this process. The CyberPeace Institute stands ready to inform these negotiations in its expert capacity as an accredited non-governmental organization to the Ad Hoc Committee.

---

[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] See Draft Text of the Convention here: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main
[3] The Humanitarian Cybersecurity Center is a partnership platform that scales up cybersecurity solutions for humanitarian NGOs. The Center provides expert support and practical assistance to NGOs that is tailored to their needs, and available globally. This work builds upon the CyberPeace Institute's key capabilities and develops programs of activities and associated projects to support communities vulnerable to threats in cyberspace. More information about the Humanitarian Cybersecurity Center: https://cyberpeaceinstitute.org/humanitarian-cybersecurity-center/
[4] More information about the CyberPeace Builders program is available here: https://cyberpeaceinstitute.org/cyberpeace-builders/
[5] International Telecommunication Union (ITU), "Bridging the gender divide," available at: https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx
[6] 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
[7] 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
[8] See the consolidated negotiating document here: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main
[9] More information on conditions and safeguards in Article 15 of the Budapest Convention: https://www.coe.int/en/web/cybercrime/the-budapest-convention
[10] As agreed in the 2021 OEWG Final Report, A/75/816, paragraph 56
[11] UN General Assembly resolution (A/RES/75/282) can be found here: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement