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

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

CyberPeace Institute's Submission to the Fifth 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 welcomes the openness and inclusiveness of this process agreed upon in the modalities of the participation of multi-stakeholders. We appreciate the opportunity to provide comments on the "Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes."

For the fifth session of the Ad Hoc Committee tasked to elaborate the cybercrime treaty, the Institute offers the following recommendations for States. These recommendations aim to contribute to the development of a document that can serve as a practical law enforcement and legal tool with the overarching goal of enhancing international cooperation and underpinning the protection of human rights in combating cybercrime.

Focus on the victims of cybercrime

States have engaged in negotiating a future convention on cybercrime amid a rapid change in the cyber threat landscape. Malicious actors target critical infrastructure and vital services with a growing frequency, scale and sophistication increasing the risks, negative impacts and harm to people. Cyberattacks against critical infrastructure, services and organizations affect people both online and physically. In the preamble, recognizing the diverse, global experiences of cybercrime victims is significant in terms of justifying the purpose and relevance of a new international instrument.

The preamble acknowledges that States are concerned by the increase in the rate and diversity of crimes committed in the digital world and its impact on the stability of critical infrastructure as

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

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

well as the well-being of individuals and society. This section further recognizes the growing number of victims of cybercrime and the importance of obtaining justice for those victims. This is a key statement as the main purpose of a new international treaty on cybercrime should be to protect and bring remedy to its victims through evidence-led accountability, allowing those affected by cybercrime to seek redress and for measures to prevent their re-victimisation.

The preamble should further consider different kinds of harm inflicted by cybercrime. This can be achieved by stressing the impacts on people who are disproportionately targeted or affected in cyberspace and the differentiated impacts of cybercrime they may experience. 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.

Decision makers must enhance their understanding of the harm on cybercrime victims, including specifically vulnerable and targeted groups. Adopting a victim-centric approach to drafting the convention can allow for an evidence-based assessment of the impacts and harm of the proliferation of cybercrime on victims and the impact of anti-cybercrime measures. Correspondingly, designing specific and adaptable mechanisms to protect human rights, with particular attention to the needs of vulnerable groups, will be critical for ensuring a positive societal impact in the future implementation of the instrument.

Mainstreaming the victims' perspectives throughout the chapters on preventive measures and technical assistance can support the development of targeted, needs-driven, and context-specific responses to mitigating and preventing cybercrime. Moreover, the periodic review of the convention's impact and implementation through a Conference of State Parties or other measures could be more accurate, informed and sustainable through the inclusion of the expertise and perspectives of human rights and civil society organizations that work in proximity with cybercrime victims.

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

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

Ensure protection of human rights

A convention must serve as a practical law-enforcement tool whilst ensuring full respect for human rights including robust protections and safeguards. Adopting a human-rights-by-design approach would be important in this regard. This approach recognizes the need to support the operational and practical priorities in preventing, combatting, and deterring cybercrime by acknowledging the significant human dimension of cybercrime. In this way, the instrument can proactively prevent potential risks to human rights. A new treaty needs to ensure that human security, equity and dignity are protected in line with state obligations towards their citizens as well as with the established international human rights frameworks.

We welcome the reference in the preamble to the commitment of States to promote 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. This is an important recognition of the language that should be further strengthened by references to specific human rights frameworks such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

The preamble continues by stressing the need to ensure a "balance" between the interests of law enforcement and respect for human rights. Whilst this language reflects other international agreements, it is important that fighting cybercrime does not pit national security against human rights. A rights-respecting and rights-protecting legal instrument should emphasise that these terms are mutually supportive. This framing is especially significant because governments have long exploited cybercrime measures to expand state control, broaden surveillance powers, restrict and/or criminalise freedom of expression and assembly, and infringe on privacy.

The recent rise in the use and mis-use of cybercrime instruments and legislation by some states to target human rights defenders, journalists, or opposition citing national security concerns, maintaining social order, and fighting terrorism is alarming. Such references must be prevented

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

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

across the convention, importantly in the scope of criminalization, but also in the chapter on international cooperation, namely its provisions on extradition and the request for mutual assistance. The principles of dual criminality are necessary to prevent the potential of persecution or other human rights violations. In this regard, the stipulation that the requested State Party can refuse extradition should there be substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of a person's characteristics in Article 58 (15) is important, and can be further strengthened by outlining additional features, especially gender.

A new cybercrime treaty cannot become an avenue for states to reduce their existing obligations under international law, especially international human rights law. In that spirit, the treaty must maintain, add to, or streamline existing international legal obligations. It is also important that the safeguards provided in the treaty are stipulated throughout the document in their entirety, as some provisions, for example, in Articles 61, 68, 69 would benefit from stronger guarantees. While these articles include recognition that the powers and procedures provided for in the chapter on international cooperation are subject to the conditions and safeguards provided for in Article 42, this guarantee may prove insufficient for the protection of human rights dependent on the final text.

It is paramount that this convention, which has the potential to profoundly impact millions of people around the world, makes it clear that powers and obligations of state agencies engaged in fighting global cybercrime reinforce and not endanger or undermine human rights. To this goal, the chapters on technical assistance, the mechanisms of implementation and the final provisions should commit to respect for human rights and fundamental freedoms, be inclusive and non-discriminatory. They need to include additional references to international human rights law and standards and to resolving challenges in a way that mitigates risks to human rights should they arise. This would solidify the importance of States considering international human rights law obligations in the implementation of the convention, as opposed to only in accordance with its domestic law.

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

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

Terminology

Acknowledging that cybercrime is rapidly evolving in terms of tools and practices, and that definitions need to be adaptable, the terminology of the convention must serve two purposes – to clearly define the scope of crimes covered in the convention and to do so in a technology-agnostic way. 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.

Determining terminology in any legally binding instrument requires careful consideration of the context and consequences of its implementation. This is especially important in a criminal justice treaty aiming to advance cooperation between law enforcement globally. Such text requires that criminalization and obligations for international cooperation are precise, accepted, and clearly understood across jurisdictions. This is also a prerequisite for ensuring that the provisions in the treaty will not come in conflict with or undermine human rights. Narrowing the definitions to what is legitimate, necessary, and proportionate will help to avoid overbroad interpretations and support effective international cooperation.

Furthermore, States need to reduce the unnecessary, confusing, or unclear terms in the treaty and make explicit references in the text that are established in existing legal instruments and therefore provide grounds for harmonisation of new and existing frameworks. For example, the term cybercrime has been tried and tested in the Budapest Convention and enjoys a broad recognition across States and stakeholders. Referring to “the use of ICTs for criminal purposes” can lead to overbroad definitions and include a diverse set of technological tools and resources that do not correspond with the core cyber-dependent crimes that should constitute the backbone of the future instrument.

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

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

Multistakeholderism

A multistakeholder approach is key to effectively addressing the challenges of transnational cybercrime. This has received an acknowledgment in the modalities of multistakeholder engagement as well as during the negotiating process itself. Current attackers in cyberspace are not guided by a silo approach and all relevant stakeholders must work together to prevent and counter their actions. Therefore, it is important that in combating cybercrime the need for cooperation between States and civil society, academia and industry, while already listed in the preamble, is highlighted in a separate point and not attached to the need to protect legitimate interests in the use and development of information technology.

Public-private partnerships are key to facilitating, supporting, and enhancing the investigation of cybercrime. States need to reduce the operating space for criminals, by implementing agreed-upon international legal frameworks, streamlining investigations and prosecutions, and also by incentivizing public-private partnerships. We appreciate the stipulation under international cooperation in Article 76 on public-private partnerships to enhance the investigation of cybercrime that States should streamline cooperation with industry and the need for an enhanced collaboration. However, considering the diverse legal and regulatory environment for private service providers across jurisdictions, it is necessary to add a reference to full respect for human rights in the guidelines for service providers in assisting law enforcement agencies in the investigation reflecting on the human rights obligations outlined above and the UN Guiding Principles in Business and Human Rights that serve to prevent, address and remedy human rights abuses committed in business operations.

The mechanisms of implementation of the convention on cybercrime must reflect the multifaceted cybercrime landscape. The openness and inclusiveness of this process and the active participation and views put forward by stakeholders during the drafting of the convention create trust between Member States and the involved organizations and experts, which will be critical in its implementation. We appreciate that Article 94(6) outlines that the Conference of the

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

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

State Parties will also consider inputs received from relevant non-government organizations. We further recommend that the commitments to human rights and guarantees for ongoing multistakeholder engagement are stipulated in the document in points on the periodical review of the implementation of this Convention (Article 94(4)). In line with this, the final provisions need to reflect on the existing modalities for stakeholder engagement and the open, inclusive and transparent nature of the participation should be also translated into the possible negotiations of additional protocols.

Conclusion

The CyberPeace Institute stands ready to inform the negotiations in its expert capacity as an accredited non-governmental organization to the Ad Hoc Committee. This process has been in many aspects a model of the effective inclusion of stakeholders. However, as the negotiations move forward States need to sustain and intensify this engagement. Building active and formal channels of communication are necessary for increased transparency, especially as some core discussions have moved to informal working groups allowing only state participation. Civil society, industry, academia, and other experts can play an important role in reaching a consensus and helping the treaty's adoption and implementation.

Countering cybercrime needs a whole society approach. Our collective goal is to ensure that human rights and fundamental freedoms are always prioritised when countering cybercrime, including in securing electronic evidence, facilitating international cooperation, and providing technical assistance.