Revisiting the Multistakeholder Manifesto at the 11th Hour

The 2021 Multistakeholder Manifesto has united the cybersecurity community in calling on states engaged in the cybercrime negotiations to prioritise protecting victims; improving international cooperation; protecting human rights and existing international law; incorporating safeguards and accountability mechanisms; future-proofing the treaty; and maintaining an open, free, and trusted Internet.

The CyberPeace Institute and the Cybersecurity Tech Accord have actively participated in the work of the UN Ad Hoc Committee tasked with drafting the Cybercrime Convention. While progress has been made, the revised draft of the treaty is concerning as it undermines the principles outlined in our original Multistakeholder Manifesto.

We regret that the substantive input provided by the stakeholder community has not been reflected in the current draft. Without significant changes, this Convention will facilitate, rather than reduce, cybercrime by significantly weakening cybersecurity, eroding data privacy and trust, increasing conflicts of laws, and undermining online rights and freedoms across the world. We urge states to adhere to the principles outlined in our Manifesto, which are today ever-more relevant for shaping a new cybercrime treaty in line with protecting human security, equity, and dignity in cyberspace.

Protect Victims

The main purpose of a new international law against cybercrime should be to protect victims, offer effective remedies, and provide human rights safeguards. We have called for prioritising 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 not contain effective protections. 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 community. We request the text be revised to require robust protections for victims in line with international standards and human rights law.

Combat Cybercrime through International Cooperation

The primary purpose of a new UN Cybercrime Convention should be to combat cybercrime across the world. States must prevent potential misuse of the Convention as a tool for governments to weaken their existing obligations under international law. The draft treaty deviates from its original aim and is designed as a "digital surveillance treaty" with proposals that expand government access to personal data. It allows for digital surveillance and an unprecedented access to personal data located in third states, without the knowledge of such states or impacted individuals. This will undermine trust in the digital environment. We call on states to guarantee the highest standards for the protection of personal data and ensure that government agencies transmit personal data on clearly defined terms and in accordance with established international standards. The principle of dual criminality needs to be embedded in the treaty to ensure that international cooperation is not used as a tool for political or other repression.

Uphold International Legal Obligations

A new cybercrime treaty must not reduce states' existing obligations under international law, especially international human rights law. We have urged states to build on existing international and regional instruments to facilitate greater cooperation in combating cybercrime. Unfortunately, the current text selectively quotes from existing treaties, lacks meaningful safeguards, and introduces troubling new text that could harm human rights online. This will prevent effective international cooperation as countries with different standards for data protection will not be able to transmit personal data to other jurisdictions that do not fulfil these requirements. We call for stringent safeguards that can facilitate and streamline cooperation between state agencies to effectively combat transnational cybercrime while ensuring that human rights and freedoms are respected and protected.

Focus on Accountability

A new Convention should enable victims to seek redress and hold actors responsible for crime accountable. States must deny safe havens used to evade prosecution by those who engage in cybercrime. The current text does not adequately reflect these requirements and does not guarantee return of proceeds of crime to victims. We call on states to limit jurisdictional frictions and implement

robust safeguards to allow data custodians to share electronic evidence in observance of the international human rights standards.

Future-proof the Treaty

The scope of the Convention must be clearly defined in a technology-agnostic way to account for the rapidly evolving nature of cybercrime. The Convention must avoid terms that could extend its application beyond cyber-dependent crime and focus on clear and precise terms that support effective implementation. We are concerned that references in the revised draft could expand criminalization to consider any activity involving the use of ICTs. Determining terminology in any legally binding instrument requires thorough and highly technical legal discussions that take into account the entire text and context of the instrument. This is especially important in the context of a criminal justice instrument, so that criminalization and international cooperation obligations are clear and precise. We propose to use the term "cybercrime" which has been tried and tested in other legal frameworks and enjoys a broad recognition across the international community.

Preserve an Open Internet

A future cybercrime Convention must not provide justification for any state to further endanger the open internet by closing off their digital borders in the name of preventing cybercrime. The draft treaty excessively defers to domestic laws, which may lead to fragmentation of the existing Internet governance framework. We urge states to uphold international standards, especially international human rights standards, and ensure that the treaty's outcome unequivocally supports and promotes a free, open, secure, stable, accessible, interoperable, and peaceful cyberspace for all.

Pursue a Systematic Multistakeholder Approach

Meaningful multistakeholder consultations and involvement should be present throughout the process. The Committee sets a welcome precedent for stakeholder inclusion in UN processes on cyber and tech related issues. However, this formal openness did not translate into an actual impact. Stakeholders' input and views were not reflected in the drafting process. We call on states to thoroughly consider the suggestions made by the multistakeholder community in a more constructive manner.

Promote Transparency

Negotiations and the following implementation of the proposed treaty must be as transparent as possible. Trust between states and the stakeholder community will be critical for the implementation of this instrument. Given the important roles of civil society, industry, academia, and technical experts, their systematic and substantive engagement should be reiterated in the mechanism of implementation. We encourage putting forward a clear set of principles supporting stakeholder participation that can ensure inclusivity, transparency and efficiency of the envisioned mechanism and ensure an effective oversight of the implementation.

Clarify the Scope of the Convention

An overly broad definition of cybercrime, as currently included in the Convention, will criminalise a wide range of activities that goes far beyond cybercrime and threaten to violate rights and freedoms. As it stands, the draft treaty could eventuate into human rights violations, especially in the areas of privacy and freedom of expression. We call on states to limit activities covered under this Convention to a clearly and narrowly defined scope of activities that enjoy strong consensus among states and are paired with adequate standards and safeguards. We further propose that the text makes clear references to the necessity of "criminal intent" to avoid victimising individuals who do not intend to cause any harm or damage. Legitimate activities of ethical hackers, cybersecurity researchers, and pen-testers that keep the digital ecosystem secure must be protected.

Pursue a Consensus-driven Approach

A new cybercrime treaty should be the product of a consensus-driven approach. Unfortunately, throughout the negotiations, states have disagreed on far more than they have agreed on with some states deciding to abandon the search for consensus completely. The collective goal must be to design a UN instrument that acknowledges that combating transnational cybercrime and protecting people's rights and freedoms are two mutually supportive goals – allowing for investigating and prosecuting cybercrime more effectively.