Multistakeholder Manifesto

Prioritizing Human-Centric Equities within the Proposed UN Cybercrime Treaty

The cyber threat landscape is in a period of rapid change, as a rise in the frequency, sophistication, and intensity of attacks threaten our collective security. Cybercrime poses new risks to human security, dignity, and equity. No single actor can adequately counter them on their own. A multistakeholder approach is vital to addressing the transnational challenges of malicious use of information and communication technologies (ICT) and to protecting and empowering its users.

We are closely following the negotiation process of the new cybercrime convention, as established by United Nations General Assembly resolution 74/247. Given the existing international and regional instruments to combat cybercrime, we urge the international community to avoid duplication of efforts and focus on efforts to strengthen the implementation and enforcement of established frameworks.

Nevertheless, recognizing the majority vote in the United Nations, we lay out a set of principles that we believe the participants to the process should follow to underpin rights and liberties that are needed to achieve a free, open, secure and peaceful cyberspace, and strengthen the respect for rule of law in cyberspace.

Protect Victims

The main purpose of new international law against cybercrime should be to protect targets and victims of cybercrime, offer effective remedies and an adequate set of human rights safeguards. Governments around the world have long abused cybercrime measures and used cybercrime legislation to expand state control and criminalize the publication and dissemination of unwelcome content, to impose mass surveillance and curb privacy in the name of fighting terrorism. A new treaty needs to ensure that human security, equity and dignity are protected, in line with state obligations towards their citizens. To protect the victims of cybercrime, any future legal instrument should ensure that definitions qualifying behavior as criminal are constructed with an adaptable, yet narrow scope to prevent criminalization of behavior that constitutes the exercise of fundamental freedoms and human rights.

Effectively Combat Cybercrime By Enforcing International Cooperation

The primary purpose of any new UN cybercrime convention should be to combat cybercrime while prioritizing human-centric equities. Effectively applying existing solutions to enforce international cooperation between the judiciary and law enforcement under transparent oversight and respecting human rights should be the cornerstone of the new treaty. The treaty should recognize that investigating and prosecuting cybercrime necessitates increased cross-sector and international collaboration, as well as harmonization of frameworks.

Maintain Existing International Legal Obligations

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, a new treaty must add to or streamline, rather than replace, existing international legal obligations upon states. Any new treaty should reinforce existing international legal obligations and be based on a clarification of the positive impact of these treaty obligations.

Focus On Accountability Mechanisms

Any new convention should focus on evidence-led accountability, allowing those affected by cybercrime to seek redress and remedy. States need to reduce the operating space for criminals, not only by implementing agreed upon international legal frameworks, working with each other on prosecution, but by incentivizing public-private partnerships to fight cybercrime. The impact of cybercrime on society as a whole should be considered, when holding those responsible for harm accountable.

Timeproof Any Treaty

Acknowledging that cybercrime is rapidly evolving, and definitions might need to follow suit, the scope of any convention must be clearly defined in a technology-agnostic way.

Preserve An Open Internet

Increasing number of countries are pursuing the objective of splintering the Internet into various national spheres of influence and control. Any new cybercrime convention must not provide justification or pretext for non-democratic regimes to further endanger the open internet by closing off their digital borders to the rest of the world in the name of preventing cybercrime. To ensure an open Internet the new treaty should ensure it sets up for adjusting jurisdictional rules to account for the reality of globalized internet and free flow of information.

ESTABLISHING THE RIGHT PROCESSES

Pursue a systematic multistakeholder approach

At all points in the process, there should be meaningful multistakeholder consultation and involvement. The equities of civil society, industry, academics, researchers, technical experts, and scientific and research institutions must be included and considered. To strike the right balance in these negotiations, experts in cybersecurity, Internet governance, international law, and human rights, among other subjects, should be at the table.

Promote transparency

Negotiations over the proposed treaty should be as transparent as possible. Organizations, individuals, and states whose equities and rights may be affected by the negotiations should have the opportunity to respond and to be heard. The schedule of and participants in negotiation sessions should, for example, be made available to the public, as should any draft texts.

Clarify the scope

An overly broad definition of cybercrime has the potential to criminalize an expansive set of activities that goes far beyond actual cybercrime. Negotiators should be careful to clarify the scope of the relevant crimes they seek to punish to ensure that this treaty cannot be used to justify crackdowns against political opposition, human rights defenders, or civil society.

Adopt a consensus-driven approach

Any new cybercrime treaty should be the product of a consensus-driven approach.The treaty should feature provisions agreed upon by a diverse range of countries and regions and based on extensive consultations from relevant experts and stakeholder groups.

Signatories:

7amleh
The Arab Center for Social Media Advancement

Africa Freedom of Information Centre

Asia Internet Coalition

Atlassian

The Azure Forum for Contemporary Security Strategy

Castroalonso LET

Center for Democracy and Technology

Cyber Governance and Policy Center
at the University of Oklahoma

Cyber Project at the Belfer Center

Cyber Threat Alliance

CyberPeace Foundation

CyberPeace Institute

Cybersecurity Advisors Network (CyAN)

Cybersecurity Tech Accord

CyberSolace Limited

Cyberspace Cooperation Initiative
at Observer Research Foundation America

Derechos Digitales

Digital Peace Now

Diplowomen

Dragos

ESET

FIRST

Fundación Karisma

F-Secure

GitHub

HackerOne

Hitachi

Identity Valley

Institute for Security and Technology

International Service for Human Rights (ISHR)

Internet Sans Frontieres

Jokkolabs Banjul

Media Matters for Democracy

Microsoft

Myanmar Center for Responsible Business

Luta Security

NetApp

Ostrom Workshop Program on Cybersecurity and Internet Governance
Indiana University

Packet Clearing House

Paradigm Initiative

R Street's Cybersecurity & Emerging Threats

Ranking Digital Rights

Rapid7

Redes Ayuda

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa

Silverado Policy Accelerator

Tech Policy Design Centre
Australian National University

The Centre for Internet and Society

USM Technology

Wisekey

World Wide Web Foundation
via The Contract for the Web

Luca Belli
Director of the Center for Technology and Society at Fundação Getulio Vargas

Vinton G. Cerf
Vice president and Chief Internet Evangelist, Google

Fergus Hanson
Director, International Cyber Policy Centre

Katie Moussouris
Founder and CEO, Luta Security

Marc Rogers
Founder, CTI League

Anne-Marie Slaughter
Bert G. Kerstetter '66 University Professor Emerita of Politics and International Affairs, Princeton University

Cris Thomas
Security Researcher, Space Rogue

Christopher Painter
President of The Global Forum on Cyber Expertise Foundation, signing in personal capacity.

Eneken Tikk
Cyber Policy Institute