Open letter to the Chair of the Ad Hoc Committee on Cybercrime

February 8, 2024

Your Excellency,

Our organizations – spanning civil society, industry, and the technical community – wish to urgently draw your attention to critical flaws in the latest draft of the UN cybercrime treaty. While we have diverse perspectives and often do not agree on a range of other policy issues, we share profound concerns over these critical shortcomings. As members of the multistakeholder community we could only support developing a treaty that would effectively address cybercrime and foster international cooperation in accordance with international human rights law and the rule of law in general. While we understand that the text is an attempt to synthesize the views of negotiating states, the result is a draft treaty that would make cyberspace less secure for everyone. The organizations signing this letter, who come from across the multistakeholder community, are deeply concerned by the adoption of such a flawed treaty without major changes.

Serious flaws of the latest draft include an unclear and overly broad scope, vague criminalization provisions and definitions, lack of meaningful human rights safeguards and effective gender mainstreaming, missing protections for good-faith cybersecurity researchers and others acting in the public interest, and overly broad provisions for real-time interception of content and traffic data that go far beyond what can reasonably be justified to fight cybercrime.

Particularly concerning is that the draft treaty authorizes states to conduct intrusive cross-border data collection without prior judicial authorization, without oversight, and in secrecy. Service providers would be unable to notify users or inform anyone about data collection being ordered. Civil society and individuals would not know when their data is being accessed, making it impossible for them to challenge arbitrary requests and protect their privacy. Given these flaws, this process is at real risk of producing an instrument that can be used to conduct broad data collection on a global scale under the guise of fighting cybercrime.

If adopted without major changes – changes we have consistently advocated for throughout the process – the risks of this treaty far outweigh its potential benefits. Notably, some elements of the treaty do not include any human rights safeguards at all, while other provisions would allow states considerable latitude to implement these safeguards. Allowing individual states to arbitrarily define what activities fall under the treaty's scope would also inevitably lead to human rights violations and criminalize legitimate activity. Individuals, including political dissidents, journalists, human rights defenders, and those at risk of discrimination on the basis of their personal characteristics would face the risk of being subjected to investigations leveraging the procedural measures of this proposed treaty without notice, potentially resulting in extradition and prosecution for exercising fundamental human rights while using digital technology. Such an outcome – facilitated by an instrument adopted by the UN General Assembly – would damage UN credibility and legitimize state behavior that undermines the rule of law while eroding respect for human rights

To make matters worse, the proposed treaty would weaken global cybersecurity and make both individuals and institutions less safe and more vulnerable to cybercrime, thereby undermining its very purpose. Expansive concepts of what activity may be subject to this treaty – and its significant procedural powers – create an unpredictable legal environment that will discourage critical security research. It may

also subject good-faith security researchers, IT professionals, and journalists to criminal prosecution for cybersecurity work that keeps us all safer. The resulting environment would make it easier for malicious actors to create and exploit weaknesses in the digital ecosystem. This could, in turn, lead to an increase in the common harms suffered in connection with cyberattacks, such as unauthorized disclosure of personal information and the disruption of access to important networks and systems, including critical infrastructure.

Furthermore, the increased risk of this treaty facilitating broad government data collection without strong privacy, due process and human rights safeguards may deter individuals and groups from exercising their rights to free speech and expression. This climate of self-censorship will have a negative effect on democratic discourse and civic participation. In essence, instead of serving one of its goals, the protection of private personal information from cybercrime, the treaty would paradoxically increase the risk of such violations and undermine human rights in the process.

A UN treaty that authorizes broad government data collection, creates an uncertain legal landscape for legitimate cybersecurity research, and facilitates greater online censorship, without sufficient guardrails as a global standard is deeply concerning. Ultimately, such a treaty would significantly erode trust and cooperation among all stakeholders, whose joint efforts are essential to address the growing global scourge of cybercrime.

Given the broad-based and fundamental concerns from stakeholders, we urge governments to consider withholding support for the treaty in its current incarnation.

Submitted by NGOS participating under operative paragraphs 8 or 9:

Access Now
ARTICLE 19
Association for Progressive Communications (APC)
CyberPeace Institute (CPI)
Cybersecurity Tech Accord
Electronic Frontier Foundation (EFF)
Derechos Digitales - América Latina
Global Partners Digital (GPD)
Human Rights Watch (HRW)
International Chamber of Commerce (ICC)
Privacy International
Red en Defensa de los Derechos Digitales (R3D)
Reporters Without Borders (RSF)
United States Council for International Business (USCIB)
7amleh - The Arab Center for the Advancement of Social media

The full list of signatories supporting the letter is available at this link.