An overbroad, unbalanced and dangerous UN cybercrime treaty must be rejected

7 August 2024. In a few days the UN is expected to agree an international treaty against cybercrime that, in its current, almost final form, poses significant risks to both human rights and the security of digital communications.

The *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is concluding its final negotiating session at UN headquarters in New York City, after over two years of negotiations which exposed deep divisions among states.

The current text is overbroad, unbalanced and dangerous.

It is overbroad as the draft treaty does not cover only cybercrime. Indeed, there is a disconnect between the crimes included in the draft treaty (Chapter II) and the scope of application of the powers to investigate crimes and to provide cooperation across jurisdictions (Chapters IV and V). For example, under the current text, powers afforded to law enforcement agencies apply to the investigation of criminal offenses committed by means of a computer system as well as the collection of evidence in electronic form of any criminal offense. Consequently, the scope of application of some of the most privacy invasive provisions is expanded well beyond cyber-dependent crimes. Arguably it makes the treaty one of the most far-reaching in criminal matters and international cooperation on criminal investigations.

It is unbalanced, as the risk of abuses that such broad scope entails are not mitigated by adequate human rights safeguards.

Articles 29 and 30 provide for real-time collection of traffic data and interception of content data, respectively. These are extremely intrusive measures that require a set of stringent limitations and safeguards, such as being limited only to serious crimes recognized under international law, following a prior judicial authorization that assessed their necessity and proportionality, including whether other less privacy-intrusive measures were not available to achieve the legitimate aim. These safeguards are not reflected in the text of Article 24, which deals with conditions and safeguards.

On international cooperation (Chapter V), the draft treaty is also very broad, covering not only the crimes listed in the Convention, but also the collection, obtaining, preservation and sharing of e-evidence of serious crimes (Article 35). When it comes to sharing of personal data across jurisdiction, Article 36 subjects transfers of personal data to domestic law and applicable international law. The article fails to provide effective protection and redress. This becomes particularly evident in jurisdictions that do not adequately regulate the processing of personal data in their national laws, or lack fundamental principles such as purpose limitation and data minimization which accordingly limit the sharing of personal data and prevent unauthorized access.

It is dangerous because the draft treaty will also make digital communications more vulnerable to those cybercrimes that the treaty is meant to address.

The draft fails to incorporate language sufficient to protect good-faith actors from criminal prosecution, such as security researchers, whistleblowers, activists or journalists. Further, the provision detailing the powers of search and seizure of information stored in a digital device (paragraph 4 of Article 28) is worded in a way that may result in states imposing obligations upon telecommunications and internet service providers to either disclose vulnerabilities of certain software or to provide relevant authorities with access to encrypted communications. This would open the door to government hacking or even undermine or weaken encryption, thereby compromising privacy and security of digital communications.

Throughout these negotiations, Privacy International and other civil society organizations, UN human rights experts, academics, security researchers and the industry have consistently recommended that any UN cybercrime treaty is narrow in scope and contains robust safeguards to mitigate the risks of human rights abuses. It is regrettable that our recommendations have not been reflected in this final draft.

As Privacy International has consistently affirmed, if the draft treaty cannot be fixed, it should be rejected. There is no longer time for negotiations to significantly improve the text.

It is now time to reject this draft treaty.