7 Oct. 2024

GNI Calls on Member States Not to Support the UN Convention Against Cybercrime

The Global Network Initiative (GNI) is deeply concerned that the **UN Convention Against Cybercrime (the UN Convention) creates a permission structure for the extraterritorial surveillance and prosecution of human rights defenders, the harassment of tech company employees, and the compelled compromise of systems that protect the privacy and security of users around the world**. As detailed further below, the UN Convention creates broad powers not previously enshrined in any other international instruments, applies to an extremely wide range of crimes "committed through the use of information and technology systems," and – despite laudable efforts to introduce human rights and effective gender mainstreaming language into the text – it fails to create meaningful human rights safeguards that would guard against its misuse.

For over a decade-and-a-half, GNI and its members have been documenting and calling out overzealous, disproportionate, and discriminatory uses of criminal authorities. Such abuses will, unfortunately, continue with or without this UN Convention, but the Convention's gravitas as a UN treaty and lack of substantive and structural safeguards would be used to justify such abuses and make it increasingly difficult for tech companies, civil society advocates, and governments around the world to push back on them.

Governments must work individually and collectively to address the scourge of cybercrime. They must also ensure that their efforts – like all investigative and prosecutorial authority exercises – are consistent with international human rights law. The largest existing gaps in international cooperation on cybercrime are not legal ones, but rather the lack of resources and capacity on the part of many individuals, organizations, and governments to understand and address these sophisticated challenges. **We call on member states to vote no or abstain when this UN Convention comes to a vote at the UN General Assembly, while bolstering resources for existing bilateral and multilateral mutual legal assistance efforts, building capacity for rule of law abiding investigation and prosecution, and improving coordination on legitimate, necessary, and proportionate efforts to address cybercrime**.

I. Overbroad Scope of Application

The Convention significantly expands the scope of cybercrime and the power of States beyond that delineated in the Council of Europe Convention on Cybercrime (Budapest Convention), increasing the potential for overcriminalization. Article 4 of the UN Convention states that any criminal act contained in any "UN conventions or protocols" should be considered covered crimes when "committed through the use of information and technology systems. This expands the traditional understanding of "cybercrime" to cover an overbroad range of non-cyber activities.

Moreover, the UN Convention definition of "technology system-related theft and fraud" in Article 13 is overly broad, leaving room for arbitrary interpretation and potential abuses. Among other things, this Article compels State Parties to criminalize "Any deception as to factual circumstances made through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do." The range of legitimate circumstances that would likely be criminalized under this provision by non-democratic countries is staggering, ranging from the ethical and legitimate conduct of research to cybersecurity penetration testing, to the publication of opinion pieces online.

Finally, the UN Convention's criminalization chapter requires law enforcement provisions and procedural measures to apply to any crime involving technology. It requires international cooperation to collect e-evidence in the case of any "serious" crime, arguably opening this obligation up to a much wider set of circumstances than those specifically delimited in the Convention's text. Serious crimes are defined as those for which domestic law imposes sentences of at least four-years, which in many countries would include many existing laws criminalizing for instance LGBTQ+ persons, sexual and reproductive rights, religious practices, blasphemy, and *lèse-majesté*. In contrast, the Budapest Convention only covers acts specifically enumerated within it and has extensive interpretative notes and a multi-decade corpus of practice and precedent that make clear its more limited focus on acts traditionally understood to constitute cybercrimes.

The Convention also puts companies and their employees at greater risk of criminal liability. GNI is particularly concerned about Articles 18 and 19, which have a broader scope than the Budapest Convention and omit important limitations. For instance, Article 19 expands the potential criminal liability of third-party platforms beyond aiding and abetting to include "the participation in any capacity… in an offense established in accordance with this Convention." Furthermore, it requires states to criminalize "any attempt" to commit a covered crime, even if unsuccessful, as well as "the preparation for an offense." The Convention's broad language creates huge legal risks for companies providing all sorts of critical and routine storage, communication, and moderation services currently provided by ICT companies.

II. New powers

GNI echoes widespread industry and civil society concerns about the ways that the UN Convention would compel States to grant themselves excessive data access-related authorities. For example, Article 28.4 of the Convention allows law enforcement agencies to demand "any person," which could include company or government employees, contractors, or service providers, to record and provide access to confidential data, secure systems, and networks, without the knowledge of their affected employers or the governments of the jurisdictions in which they are headquartered. Nothing in the UN Convention would prohibit such authorities

from breaking the kinds of encryption routinely used to protect all sorts of data for legitimate cybersecurity, data protection, and privacy reasons.

GNI has consistently argued that the best approach to evaluating state authority over tech companies, their data, and their content is through the lens of international human rights law. These principles offer a universally accepted framework that promotes the free flow of communication and data while allowing for targeted and proportionate regulation to address specific harms.

Additionally, GNI is concerned about the stringent provisions in Article 31 of the UN Convention relating to corruption and the confiscation of criminal proceeds. The Convention mandates the confiscation of criminal proceeds and any property, equipment, or other instruments used or intended for use in criminal acts, including extensive tracing of such equipment.

Due to the UN Convention's broad scope, expansive approach to the concept of jurisdiction, and detailed commitments on international cooperation, these provisions not only pose new financial and legal risks for the private sector, but would also enable and facilitate the concerning and expanding trend of transborder, rights-abusing persecution, known as transnational repression. The UN Convention provides authoritarian countries with a legal framework to pressure smaller or politically vulnerable nations into complying with their demands for data on dissidents, journalists, and human rights defenders. The UN Convention would allow these States to frame such requests as legitimate law enforcement actions, and leverage their influence to compel other nations to hand over sensitive information, with potentially disastrous consequences for human rights.

III. Lack of safeguards

The UN Convention and the Budapest Convention have significant discrepancies in their approaches to human rights safeguards. While the UN Convention permits states to implement procedural law safeguards through domestic legislation, the Budapest Convention mandates their implementation. This difference, particularly in the context of the Convention's vague language, creates a potential for states to deviate from internationally recognized best practices in protecting human rights.

Moreover, the Convention's provisions on international cooperation and private sector obligations raise significant concerns about potential abuses. The Convention allows for indefinite secret cooperation between States and requires private sector entities to fulfill all requests, regardless of their legality or impact on individual rights. This combination of perpetual secrecy and limited procedural safeguards can lead to abusive requests, particularly for companies operating internationally.

As noted above, unlike the Budapest Convention, the UN Convention does not include an explanatory report with guidance for the implementation of its provisions and safeguards. The UN Convention similarly lacks any effective mechanism for interpretation or remedy, while the Budapest Convention is regularly evaluated by the Council of Europe and the European Court of Human Rights, which are both bound by and committed to the provisions in the European Convention on Human Rights. Most critically, if passed, the UN Convention would likely be adopted by a much broader range of State Parties, some of whom are likely to interpret the provisions inconsistently with international human rights principles and generally accepted practices.

IV. Conclusion

In conclusion, the adoption of this treaty poses significant risks to criminal justice, data access, cybersecurity, the digital economy, and human rights. Its potential to criminalize legitimate activities and grant broad and excessive powers to States presents significant risks to human rights defenders, journalists, security researchers, as well as companies and their employees with differentiated impacts based on gender. The Convention's lack of adequate safeguards and its potential for abuse by authoritarian regimes make it a dangerous precedent for international cooperation.

For these reasons, GNI calls on Member States not to support the UN Convention at the UN General Assembly. Instead, Member States committed to addressing cybercrime in a manner that respects and protects human rights should encourage the General Assembly's Third Committee to refer the Convention back to the Ad-Hoc Committee for further consideration, especially around circumscribing its scope and including additional safeguards. If the Convention is voted upon, they should oppose it or abstain from supporting it, using explanations of vote to further articulate their concerns about its potential for abuse and lack of safeguards. They should also commit to providing additional funding to their own law enforcement and mutual assistance authorities, enhancing investigative and prosecutorial capacity building for and cooperation, and supporting appropriate multilateral mechanisms to address these challenges, such as the Council of Europe, the Freedom Online Coalition, and the UN Office on Drugs and Crime.