ARTICLE 19's analysis of the UN Convention Against Cybercrime

October 2024

ARTICLE 19 is seriously concerned about the Draft of the UN Convention on Cybercrime, which is pending formal adoption by the UN General Assembly later in 2024. While we agree that addressing cybercrime is important, we warn that the Draft Convention does little to actually prevent or deter transnational cybercrime. Instead, it retains several provisions that enable or legitimise the violation of international human rights law both through domestic legislation and international cooperation without the provision of adequate human rights safeguards. While several cyber enabled crimes were removed during the negotiation process, a broadly worded preamble clause combined with a future General Assembly Resolution could enable their reintroduction through the "back door." Several provisions of the Draft Convention serve as barriers for legitimate security researchers and security research, thus undermining cybersecurity and privacy worldwide. The Draft Convention also enables sweeping legal assistance between countries without providing for adequate safeguards. The Draft Convention both enables intrusive surveillance of users and does away with transparency and accountability requirements for the governments of State Parties. Finally, it legitimises and encourages the "establishment of jurisdiction" through a range of sovereign controls that violate human rights.

ARTICLE 19 urges UN member states to not sign and ratify this Convention or use it as a template for designing domestic cybercrime legislation.

Cybercrime has emerged as a significant global threat, posing serious challenges to individuals, businesses, and governments worldwide. As digital technologies become increasingly integrated into people's daily lives, the potential for malicious actors to exploit vulnerabilities in computer networks and systems has grown exponentially. While addressing cybercrime is crucial for protecting people's rights and livelihoods, in ARTICLE 19's experience, cybercrime legislations often serve as instruments enabling the violation of international human rights law by states under the guise of furthering national security or ensuring public order.

After three years of negotiations, on 9 August 2024, the UN *Ad Hoc* Committee finalised the draft of the United Nations Convention against Cybercrime (the Draft Cybercrime Convention). The treaty negotiations were initiated by Russia and were legally enabled by a 2018 General Assembly Resolution that set up an *Ad Hoc*

Committee to carry out these negotiations. While the United States, the European Union and several other countries initially opposed the treaty and the negotiation process, they have since participated in the seven rounds of the negotiation process. The draft of the Cybercrime Convention is now to be submitted to the UN General Assembly for formal adoption later in 2024.

ARTICLE 19 has been actively participating in the negotiations process and issued comments on the earlier drafts. In this brief, we build on our earlier analysis and demonstrate why the Draft Cybercrime Convention is problematic from international human rights law perspective.

At the outset, ARTICLE 19 warns that the Draft Convention does little to actually prevent or deter transnational cybercrime or increase cyber security. Instead, it aims to reconfigure sovereign controls over a global and open internet and enable governments to use these controls to violate the rights of their citizens.

While several provisions of the treaty are worded using non-mandatory language such as "may," we are concerned that the inclusion of such voluntary provisions serves as a model for several countries that have not yet adopted domestic cybercrime legislation. In essence, it allows the legitimisation and export of rights-violating domestic legislative provisions. At the same time, it enables and in certain cases obliges cross-border cooperation between countries that do not uphold the same international human rights standards domestically, thereby starting a race to the bottom.

ARTICLE 19's key concerns with the Draft Cybercrime Convention

1. Failure to incorporate effective and specific human rights safeguards

The Draft Cybercrime Convention fails to incorporate human rights safeguards for the broad range of cross-border procedural and law enforcement measures that it enables. We note that Article 6 is an all-encompassing human rights clause which states that "nothing in this Convention shall be interpreted as permitting the suppression of human rights or fundamental freedoms." While this is an important safeguard in theory, the provision itself and the other provisions of the Draft Convention are not robust enough to ensure that the rights of individuals and users are protected for the following reasons:

- **Wording of human rights safeguards clause is inadequate:** Article 6(1) limits human rights safeguards in the Draft Convention to member states' "obligations under human rights law." Essentially, this means that states that have not signed or ratified other human rights conventions but are party to the Cybercrime

Convention are not bound by international human rights law when acting in pursuance of the provisions of the Convention.

Article 6.2 rectifies this somewhat and identifies some core human rights including the rights to the freedom of expression, conscience, opinion, religion or belief, and peaceful assembly and association. However, the right to privacy and the right to equality and non-discrimination, both also core components of international human rights law, are not a part of this list. As we outline below, several provisions could negatively impact these rights as well.

- **There are no specific human rights safeguards across various provisions of the Draft Convention:** Even if the flawed general safeguards clause was more robustly framed, we are concerned it would not be effective without the inclusion of specific human rights safeguards incorporated into various rights-infringing provisions of the treaty. We find that including specific safeguards is absolutely necessary to ensure the protection of human rights. Rights-violating conduct in pursuance of any of the treaty provisions would be undertaken by a law enforcement official of a certain State. Even if the victim of rights-violating conduct finds out about this and wants to challenge it, the only authority would be a domestic court of law or a regional human rights tribunal. While Article 6 and applicable international human rights law may be useful in that judicial context, they will not be able to prevent specific rights-infringing activity carried out in pursuance of the provisions of this Draft Cybercrime Convention in the first place. In this brief, we will further demonstrate the range of provisions where the absence of safeguards could turn them into rights-violating instruments.

2. Broad scope of preamble and potential for introducing more "cyber enabled" crimes through the backdoor

In the analysis of the previous versions of the Draft Cybercrime Convention, ARTICLE 19 raised concerns about numerous cyber enabled crimes. Cyber enabled crimes are crimes that can be committed without information and communications technology (ICT) but could be enabled through the use of ICT. Cyber dependent crimes on the other hand are crimes that cannot be committed without the use of ICT systems, such as illegal access to a computer system or illegal interception.

Although the number of cyber-enable crimes in the Draft Cybercrime Convention have been significantly reduced since previous versions, there is no clarity on the definition or threshold of the offences that may constitute a cybercrime. For example, paragraph 3 of the Preamble notes several "cyber enabled crimes" including terrorism, and transnational organised crime such as trafficking in persons, the smuggling of migrants, the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, drug trafficking and trafficking in cultural property.

Given that these crimes were removed from the operative clauses of the Draft Cybercrime Convention, their retention in the Preamble provides legitimacy for countries to criminalise them in domestic legislation or even through the Draft Convention through subsequent Protocols. In particular, the inclusion of "terrorism" as a crime in the Preamble is problematic given that there is no universal consensus on the definition of terrorism, and the amorphous idea of "terrorism" has been used to justify states' abrogation of international human rights law in a range of contexts, in particular in combating terrorism and the war on terrorism.

Further, we also note with concern that Article 21 legitimises domestic legislation that adds aggravating circumstances in order to increase the sanctions associated with a particular offence. In particular, it adds the phrase "including circumstances that affect critical information infrastructure." Given that the criminalisation of attacks against critical information infrastructure (CII) was removed as a crime in its own right over the course of the negotiations, we find it disappointing that it has been added as an aggravating circumstance through another provision. Elsewhere, we have already investigated and explained how domestic legislation dealing with critical information infrastructure could be used to stifle freedom of expression and the right to privacy of a range of business entities, including business entities and online platforms (e.g. in Hong Kong).

This enlargement of the scope of criminalisation is further enabled by a draft General Assembly Resolution linked with the Draft Convention. This resolution mandates the Ad Hoc Committee to commence negotiations on a Supplementary Protocol in order to include additional criminal offences. This would include a number of other offences (terrorism, blasphemy) that do not have universal definitions and would represent an even greater threat to human rights around the world.

3. Barriers for legitimate security research and security researchers

ARTICLE 19 also warns that various provisions of the Draft Cybercrime Convention will have negative impacts on the legitimate work of security researchers. We would especially like to highlight the following issues:

- Articles 7 and Article 8 of the Draft call for the criminalisation of illegal access and illegal interception respectively. We find the phrase "without right" to be an extremely ambiguous and broad threshold for criminality. Apart from hindering "good faith security" research, this provision could end up criminalising minor civil infractions like violations of private terms of service (TOS) contracts. Articles 7(2) and 8(2) clarify that a State "may" require such offences with the intent of obtaining electronic data or other dishonest or criminal intent. Now, the establishment of *mens rea* or criminal intent is a mandatory requirement for any

crime. Article 7 violates this fairly basic threshold as it ends up making criminal intent optional and enables states to bring within the ambit of criminality a far broader range of activities (including conduct categorised as civil violations) undertaken "without right."

- Article 9 criminalises interference with electronic data. Again, Article 9(2) stipulates that a State "may" require serious harm to accrue in order for an offence to be constituted. Security researchers often simulate cyber-attacks through such interference to test computer systems – an activity that could be criminalised through the Draft Cybercrime Convention.

Given the significant barriers to security research that the various provisions of this Draft Cybercrime Convention pose, the "recognition" of the contributions of security researchers and ethical hackers in Article 53 on preventive measures is meaningless as it does not outline any specific protection or incentives. Ultimately, this Draft Convention could have a "chilling effect" on security researchers looking to do legitimate cybersecurity work, and undermine overall cybersecurity as well as the rights of individual users.

4. There is a lack of specific human rights safeguards in procedural and law enforcement measures enabled by the Draft Cybercrime Convention

ARTICLE 19 is concerned about the absence of specific safeguards to preserve the rights to freedom of expression and privacy. We believe this omission will enable States to violate human rights law through domestic legislation enacted in furtherance of provisions of the Draft Convention. We are particularly concerned with the following provisions:

- Article 24, which provides for conditions and safeguards for the Chapter on Procedural Measures, defers entirely to domestic law. Article 24(1) specifies that domestic law must provide for the "protection of human rights in accordance with [the member states'] obligations under international human rights law} and which shall incorporate the principle of proportionality." This safeguard is grossly inadequate as it provides an extremely broad margin of appreciation for states when enacting domestic policy and allows them to selectively comply only with those human rights treaties or conventions that it has already signed. Second, the provision only mentions the principle of proportionality as a safeguard and not the principles of legality and necessity, which are legally mandated thresholds for restricting a right.

  We are also aware that Article 24(2) mentions due process mechanisms including judicial review, the right to an effective remedy, and limitation of the scope and

duration. However, yet again, it leaves the application of these provisions discretionary and contingent on domestic law.

- Article 28(4) of the Draft Convention enables legislative measures that empower competent authorities to "order" "any person who has knowledge about the functioning of the information and communications technology system in question" to provide this information to enable the search and seizure of electronic data. Notably, this provision does not include any specific safeguard protecting the right to privacy of the individual questioned. The ability to order "any person who has knowledge" about the functioning of a computer system pays scant regard to instances where the "knowledge" in question may be a trade secret, sensitive information or technical information on vulnerabilities that security researchers may be working with to conduct legitimate security research. We are also concerned, alongside other experts, that this provision may also be used to compel individuals or entities to turn over encrypted information.

- Article 29 enables states to compel a service provider with "existing technical capability" to engage in the real time collection of traffic data, again without any international human rights safeguards. Therefore, this provision essentially enables states to compel service providers to enable global bulk surveillance without any considerations for the legal standards of legality, necessity or proportionality. Given the acknowledged illegality of existing bulk surveillance programs, we find this provision specifically concerning.

- Article 30 of the Draft Convention enables even more intrusive surveillance. Article 30(b) enables domestic provisions that can compel any service provider to either collect and record themselves or cooperate and assist competent authorities to collect and record content data for specified communications within its territory. This provision does not mention checks and balances that could be provided by the judiciary such as the production of a warrant, which again provides government institutions carte blanche authority to conduct intrusive surveillance without guardrails.

- Article 47(c) encourages law enforcement cooperation for "necessary items or data for analytical or investigative purposes." We find that this amorphous phrase legitimises rights-violating law enforcement practices such as predictive policing or emotional recognition. As we and other experts warned, with the absence of privacy-protecting safeguards, it also sets the stage for sharing sensitive data and building biometric databases that could be used to disproportionately target and discriminate against marginalised communities.

5. *The Draft Cybercrime Convention provides for sweeping mutual legal assistance enabled without adequate safeguards*

ARTICLE 19 is concerned about the undermining of human rights through a framework for mutual legal assistance between countries that may not have compatible human rights frameworks domestically and may not be in consonance with international human rights law. In particular:

- As we warned earlier, Article 40(3) of the Draft Convention provides for a broad array of purposes for which mutual legal assistance may be rendered without any human rights safeguards for the right to privacy or data protection, or safeguards specifically for vulnerable persons. These include "a) taking evidence from person; b) effecting service of judicial documents; c) executing searches and seizures and freezing; d) searching or similarly accessing or similarly securing and disclosing electronic data; e) collecting traffic data in real time, f) intercepting content data, g) examining objects and sites; h) providing information, evidence and expert evaluations; i) providing originals or certified copies of business documents; j) identifying or tracing proceeds of crime; j) facilitating the voluntary production of persons in the Requesting State."

- Furthermore, Article 40(8) essentially does away with the requirement of dual criminality. The provision stipulates that States "may decline" to render mutual legal assistance, which implies that they have an option to do away with dual criminality. The provision also explicitly enables the state to provide assistance "to the extent it decides at its discretion" irrespective of whether the conduct would be a crime within its own jurisdiction.

  This provision has two impacts that negatively impact international human rights. First, if a state fails to pass domestic legislation declaring a certain offence a crime, it could still enable the harassment of individuals engaging in said conduct by rendering mutual legal assistance that enables a foreign state to prosecute that individual utilising provisions of the treaty. Second, the requesting state could exert external political or economic pressure on the requested state to render mutual legal assistance even if dual criminality is not established, thus arbitrarily enlarging the scope of criminalisation globally.

- The grounds for refusal for mutual assistance provided for in Article 40(21), on the other hand, are excessively narrow. For example, Article 40 Clause 21(b) mentions sovereignty, security, *ordre public* or other essential interests of a state but conspicuously leaves out human rights concerns as grounds for a refusal. Further, Article 40 Clause 22 exempts obligations to render mutual legal assistance only if the member state has "substantial grounds" for believing that the request has been made for prosecuting a person based on a number of protected characteristics. The

threshold of 'substantial grounds' is legally undefined but a dictionary definition of the word substantial meaning "large in size, value or importance" indicates a relatively high threshold for a refusal. Further, the protected characteristics include a person's sex, race, language, religion, nationality, ethnicity, origin or political opinions. These grounds suffer from two lacunae. First, it leaves out "sexual orientation" as a protected category. Given the number of potential member states who still criminalize LGBTQ+ communities domestically, the Draft Convention could serve as an ideal instrument to obtain data from other countries to prosecute or harass LGBTQ+ individuals. Second, the Draft Convention protects "political opinion," which is covered under the freedom of speech and expression but explicitly leaves out "political offences."

6. The Draft Cybercrime Convention fails to provide any transparency and accountability obligations on States

While various provisions of the Draft Convention give intrusive surveillance provisions to the government, several provisions simultaneously protect governments by doing away with transparency and accountability requirements, which are cornerstones of international human rights law.

ARTICLE 19 warns that this lack of transparency will prevent users from challenging acts undertaken through the Draft Convention that violate international human rights law. These provisions include:

- Article 29 (3), which enables legislative measures that oblige a service provider that is compelled to engage in bulk surveillance to keep the details of the surveillance confidential.

- Article 40 (20), which deals with mutual legal assistance, allows the State requesting mutual legal assistance to require that the details of the request be kept confidential. If the State Party executing the mutual legal assistance request cannot maintain confidentiality, it needs to inform the requesting State Party. We warn that while the confidentiality requirement here is discretionary, it perpetuates a culture of secrecy when executing key provisions of the Draft Convention, which enables governments to evade accountability.

- Article 42(3) provides that, "as appropriate," a request for preservation of user data be kept confidential by the State Party executing the request without "notifying the user."

7. The Draft Cybercrime Convention legitimises and encourages the establishment of jurisdiction through sovereign controls over the internet

ARTICLE 19 observes that Article 22 of the Cybercrime Convention encourages state parties to "adopt such measures as may be necessary to establish jurisdiction" over an offence in the Draft Convention. As we have already noted, states adopt a variety of strict technical and legal measures to exercise territorial control over various layers of the internet. These regimes include data localisation requirements, strict licensing requirements and local presence mandates for platforms, and blocking platforms that do not comply with local laws.

In essence, these measures attempt to circumvent the values of an open and global internet that enables the freedom of expression and aligns it instead with the interests of the territorial state.

Given the severe array of rights-infringing provisions in the Draft Convention itself as well as the potential use of these provisions in constructing rights-violating domestic legislation, ARTICLE 19 urges UN member states to not sign and ratify this Convention or use it as a template for designing domestic cybercrime legislation.