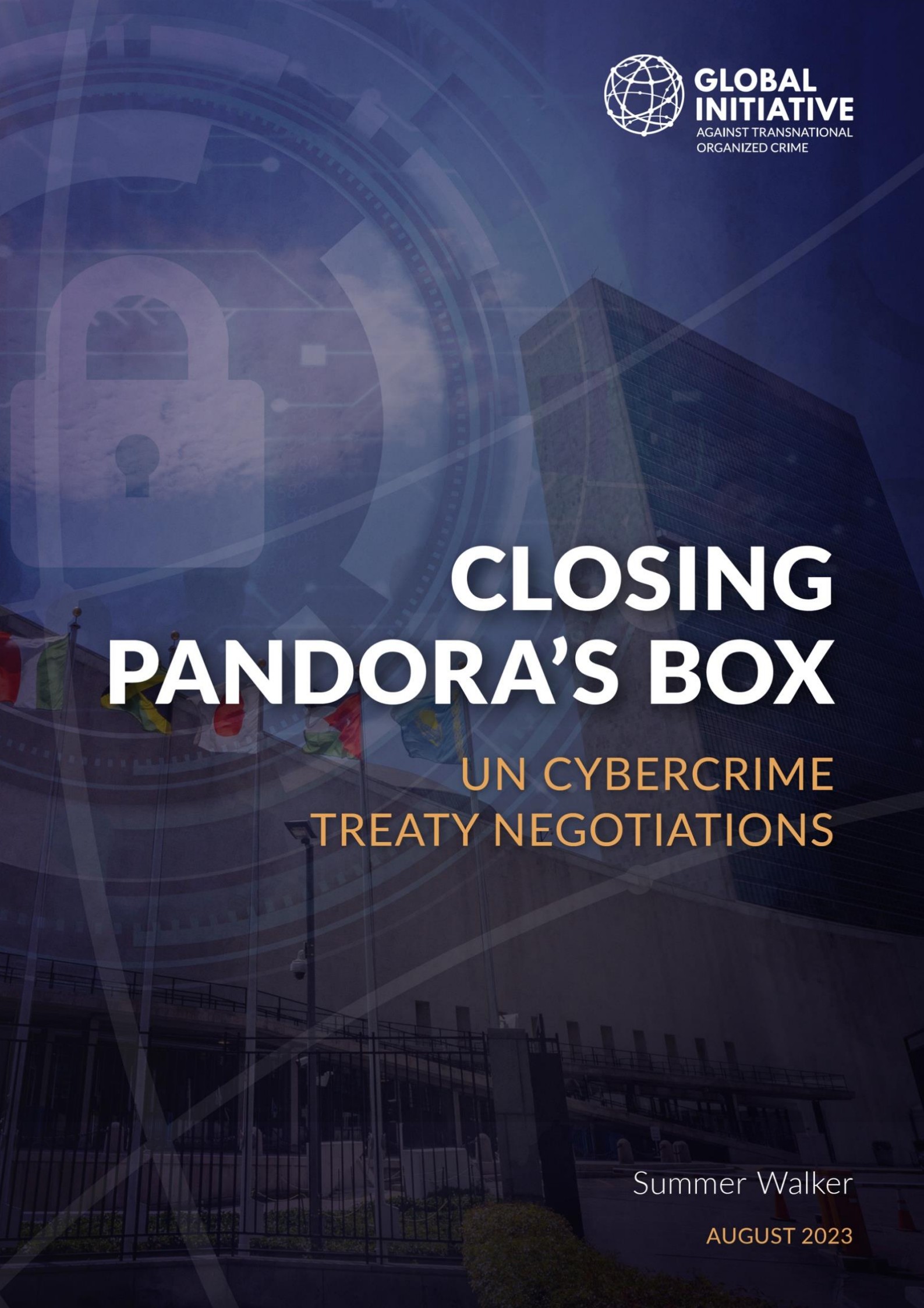

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

CLOSING PANDORA'S BOX

UN CYBERCRIME TREATY NEGOTIATIONS

Summer Walker

AUGUST 2023

NOTE

This brief is produced ahead of the sixth session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 21 August–1 September 2023, New York.

ABOUT THE AUTHOR

Summer Walker is the GI-TOC's Head of Multilateral Affairs in New York. She leads projects and provides research and analysis on international policy, with issues ranging from drug policy to cybercrime. She has worked with the UN and international NGOs, development agencies and research institutes.

Cover: © *Roy Rochlin via Getty Images*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva

www.globalinitiative.net

Contents

INTRODUCTION

A zero draft of the United Nations Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes, or more succinctly referred to as the cybercrime treaty, has been produced and will be debated in an August 2023 UN session in New York. In this context, states are debating the first global cyber-treaty, with a focus on criminality and state powers to address crime.

The zero draft document was developed from negotiating drafts that were debated over the course of this year. Overall, the secretariat of the Ad Hoc Committee established to elaborate the proposed convention has left out of the zero draft most sections where consensus had not been reached during the sessions. And in a meeting with multi-stakeholders and governments, the committee clarified that they do not plan to reinsert such sections.[1] The draft is strengthened by the removal of the most controversial provisions and of those upon which governments have thus far been unable to agree.

Throughout the process leading up to the zero draft, the Global Initiative Against Transnational Organized Crime (henceforth 'GI-TOC') submitted position statements and guidance notes, and participated in meetings with governments to discuss the content.[2] We have also communicated what we see as the greatest risks inherent in this treaty, namely its potential to advance state repression and establish new international norms that would formalize these into international law.[3]

This brief does not provide a detailed account of the draft, but focuses on two key issues that are critical to arriving at a treaty that will both increase global cooperation to combat cybercrime and, at the same time, preserve fundamental rights in the internet era. These are the need to limit the scope of crimes under the treaty, and to strengthen language around and inclusion of legal and human rights protections. This brief offers ways that governments can address these challenges in the August UN session and as the process draws to a close.

DEFINING CRIME IN AN AGE OF DIGITAL SURVEILLANCE AND INCREASING AUTOCRACY

How crime is defined in this treaty bears significance for how it will be viewed years from now. The GI-TOC has consistently argued for a narrow scope of crimes for this treaty that will enhance cooperation, but protect the treaty from becoming a Pandora's box for online and technology-enhanced government repression. In the current draft, there remain three ways of defining crime that bring real risk that this treaty will be used as a tool to support government efforts to control information and communications technology, surveil populations and normalize international cooperation for these purposes. The problematic terms in the draft are:

- 'other criminal offences committed by means of [a computer system], or [an information and communications technology device]'
- 'any criminal offence', and
- 'serious crimes'.

Below, the risks that would arise by including these terms in the final wording of the treaty are explained, including why they do not allow for sufficient protection against rights violations. Before that, it is important to clarify where these terms are found in the treaty followed by what other parameters exist for the scope of crime in the treaty.

The current draft contains a chapter that sets out specific crimes that governments have agreed should be addressed under this treaty. The draft does not include crimes for which consensus was not achieved during the rounds of debates – a decision that is supported by the GI-TOC. The abridged criminalization chapter now focuses primarily on cyber-dependent crimes (e.g. illegal access, interference with computer data, etc). It has significantly reduced the scope relating to child sexual exploitation online (e.g. child sexual abuse material) and related crimes. It retains an article on money laundering. And it includes a compromise article (offences relating to other international treaties, proposed during negotiations),[4] which asks states to adopt measures so that crimes in other conventions and protocols apply to this treaty when committed using a computer system or a digital device. Throughout the remainder of the treaty, there are distinctions made when crimes listed in Articles 1 to 16 can be applied and when crimes from Article 17 can be applied (see the table below for details). Then there are the three ambiguous crime tiers.

CRIME TIER	WHERE IT IS DEFINED IN THE DRAFT
Specific, defined crimes	Articles 1–16, Chapter II: Criminalization
Offences relating to other international treaties	Article 17, Chapter II: Criminalization; not defined in further detail
Serious crimes	Defined in terms section
Other criminal offences	Not defined
Any criminal offence	Not defined

FIGURE 1 The five tiers of crimes in the draft convention.

'Other criminal offences' and 'any criminal offence' are not defined in the treaty: they appear as part of the scope for procedural measures (Chapter IV, Article 23[5]). This is in addition to the specific, defined crimes listed in the criminalization chapter; the scope does not include any reference to Article 17. Including 'other' and 'any' offences here would allow governments to apply the treaty as justification to carry out a vast number of state procedures for any crime they deem necessary, including real-time collection of traffic data, search and seizure of stored data, or expedited preservation and partial disclosure of traffic data. Depending on the requests and the avenues for cooperation, it could allow for UN-supported cooperation in state repression of human rights, including political, social and cultural rights.

The three main references to 'serious crimes' are in Chapter V: International cooperation. Serious crimes are defined as 'conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years'.[6] The three articles are: Article 35 (General principles of international cooperation); Article 40 (General principles and procedures relating to mutual legal assistance); and Article 41 (24/7 network), which would be an operational tool to implement the convention). Each time, it is coupled with Article 17 from the criminalization chapter. Each reference relates to the collection of electronic evidence (e-evidence collection is a key objective for many member states in this treaty process). Two of these articles are under general principles sections, meaning they apply more broadly in the chapter. Serious crime may seem to be more limiting than the previous two terms, but as outlined in the next section, there are significant opportunities for it to be used for a wide variety of crimes.

Why we need revisions to the draft treaty

These three expanded scopes for crimes, as they appear in the draft treaty, are problematic for three reasons. First, a scope allowing for cooperation for other and any criminal offences or serious crimes negates the purpose of the criminalization chapter, which defines specific criminal acts. By expanding beyond a negotiated, narrowly defined list of agreed-upon crimes, implementation will likely be bogged down by governments debating how the treaty should be applied, rather than enhancing cooperation among states and across regions.

Second, they are too broad and capture a potentially unending list of crimes. By creating these open-ended boundaries for cooperation on any crime, an international treaty is likely to emerge that could permit state control over how the internet and ICTs are used in society; to increase surveillance of and advance repression against marginalized, targeted or politically threatening groups and individuals; and to extend transnational repression. And, thirdly, if the treaty were to be used to exert such control it would not be seen as a misuse of this legal instrument, but as its central purpose. It risks creating new international norms for questionable state control and surveillance of ICTs and computer systems.

Some of the language is taken from earlier negotiated text, but in today's global climate, this is the wrong approach for this treaty. Over 20 years ago, the UN Convention Against Transnational Organized Crime (UNTOC) was signed into being. In that treaty, states agreed to define serious crime as one leading to punishment of four years or more.[7] The current draft replicates this definition.

Also drafted over 20 years ago was the Budapest Convention, a cybercrime convention of the Council of Europe, which is where the language 'other criminal offences' derives from. This treaty was forged among a like-minded group of countries with similar systems for rule of law, but, as is the case with UNTOC, does not fully capture the current global geopolitical context for a treaty on cybercrime.

The ability of government agencies, corporations and even individuals to access data and surveil individuals and groups has increased exponentially over the last 20 years. People's personal details can be accessed easily online by prying agencies and authorities. Simultaneously, there has been an increasing trend towards more autocratic governance around the world, and governments, both democracies and autocracies, have shown growing interest in controlling and monitoring online activity. Finding political asylum abroad is greatly tested now by the clutches of transnational repression, by which governments silence dissent among diaspora and activists, largely using technology.[8]

The glaring risk in retaining these three terms in the text of the treaty, which either have no clearly defined parameters or are merely defined by prison terms, is the potentially unfettered scope for governments to sanction repression, which the convention would in theory legalize.

In some countries, even crimes punishable by a four-year prison sentence threshold would allow for the treaty to be used to collect data for evidence on whether a person is – for example – a women's rights activist or a political dissident. It could be used to collect evidence on activities including adultery, sex work or possession of illegal drugs purchased online, which are not criminalized in many countries, yet in others can carry long prison terms. The legal protections of proportionality and dual criminality would not stop two or more countries that collectively criminalize one of these issues to use the treaty to advance certain forms of repression or violate human rights.

For instance, the 24/7 system – an operational tool to implement the convention – could be used to compile data from dating apps to persecute LGBTQI+ individuals. Governments could produce a mutual legal assistance treaty (MLAT) request for data on participants in women's rights online forums, for example, justifying it as a public disorder crime punishable with high prison terms. They could seek data from a forum that assists women to access abortions, for instance, in countries where women's health choices incur harsh prison terms. In the United States, under its changing legal framework, in one state, Facebook/Meta cooperated – willingly – with local authorities by sharing private messages on its platform so that they could prosecute a mother and daughter who sought medicine for an abortion.[9] Imagine this type of application on a grand scale, applied across borders and facilitated by this treaty? Do governments want their stamp of approval on such a treaty, with such potentially harmful impacts on human rights?

For this treaty to be a success in implementation, it will need wide support, and for this to happen it will need to build into its provisions unbreachable protections that safeguard the rights of citizens whose governments may seek to penalize them.

RECOMMENDATION

Remove references to 'serious crimes', 'other criminal offences' and 'any criminal offences' from the draft because they are too ambiguous; they remove parameters around when and how this treaty can be used; and they create ample opportunity for treaty misuse and advancing human rights abuses through the UN system.

Article 17

Article 17 (Offences relating to other international treaties), in its current form, also lacks sufficient parameters to rein in how the treaty could be applied (for the wording of Article 17, see below). Article 17 attempts to provide a wider scope while still containing cooperation for crimes agreed upon in international law, but does not set forth which conventions and what types of crime. For instance, the UNTOC does not set out a list of crimes, although its three protocols (small arms trafficking, human trafficking and migrant smuggling) could serve as references. However, an obvious omission is that this is not clarified in the current text. The resultant ambiguity of what could be criminalized will create confusion in implementation. To give an example, while the three international drugs conventions do not criminalize personal drug use, they do not rule out its criminalization, which can carry harsh penalties in some countries. Again the issue is that governments would retain a right of refusal to cooperate based on safeguards, principles of proportionality and dual criminality – yet governments that have harsh punitive laws would be able, through the treaty, to request data from online spaces people feel are personal and protected to prosecute them.

Article 17: Offences relating to other international treaties

States Parties shall adopt such legislative and other measures as may be necessary to ensure that offences established in accordance with applicable international conventions and protocols also apply when committed through the use of [a computer system] [an information and communications technology device].

ENSURING LEGAL AND HUMAN RIGHTS PROTECTIONS

Legal and human rights protections, which have often been referred to as safeguards during the process of negotiating the treaty, are essential to this instrument's success.

They are listed in a general safeguards provisions article (Chapter IV, Article 24). Specific safeguards also appear under particular articles. For instance, Article 21 (Prosecution, adjudication and sanctions) (in Chapter II: Criminalization) says states must ensure that individuals prosecuted for offences under the crimes set out in Articles 1 to 16 are granted rights under domestic law, consistent with international human rights law, including right to fair trial and defence. And there are articles on witness and victim protection.

Nevertheless, there remains ample room for strengthening and streamlining the legal and human rights safeguards in the wording of the current draft, and recommendations on specific elements are outlined below.

For some specific articles, the draft limits the scope of application to crimes defined in the convention (Articles 1 to 16). When the draft draws these limits, it provides protections against the vast application of those particular provisions. It means they exclude crimes under other conventions, any crime or serious crimes as justification for requests for international cooperation. This can be seen in articles on extradition, jurisdiction, asset forfeiture, establishment of criminal records and protection of witnesses, among others. This distinction does not appear in procedural measures, such as preservation, and collection and sharing of computer, traffic or content data among states.

Chapter IV: Procedural measures and law enforcement

In Article 24 (Conditions and safeguards), references to necessity, legality, and protection of privacy and personal data that appeared in the previous draft have been removed. It now focuses on maintaining consistency with domestic law and obligations under international human rights law. It does not give preference to domestic law over human rights law, which is welcome. The judicial oversight clause is key to limiting cyber interventions to those that are bound by law and legal proceedings. At present, Article 24 does not apply across the draft treaty but only to Chapter IV. It should also apply to international cooperation and technical assistance, and in this respect it is recommended that it should be moved to Chapter I: General provisions, so that this provision applies across the treaty.

Chapter V: International cooperation

Chapter V does not have a chapeau article on safeguards and contains multiple ways of describing when a request for cooperation may be refused and under what conditions. In the August session, delegates should work to close those gaps to better align future interpretations of the treaty. For instance, articles listing specific actions requiring mutual legal assistance are bound by different conditions. Dual criminality is a requirement under the general principles of MLATs but it does not transfer to all of the measures below (Figure 2). Furthermore, there is no direct link or reference to Article 36 (Protection of personal data) in any of these.

MEASURE	CONDITIONS
Article 42: Expedited preservation of stored [computer data] [digital information]	Dual criminality, though not a necessary requirement. Refusal on 'basis of the grounds contained in Article 40, paragraph 21'.
Article 43: Expedited disclosure of preserved traffic data	Refusal on 'basis of the grounds contained in Article 40, paragraph 21'.
Article 44: Mutual legal assistance in accessing stored [computer data] [digital information]	None clearly stated States shall respond by 'arrangements and laws referred to in Article 35 (General principles), and in accordance with other relevant provisions of this chapter.
Article 45: Mutual legal assistance in the real-time collection of traffic data	'Governed by the conditions and procedures provided for under domestic law.' States 'shall provide such assistance at least with respect to criminal offences for which the real-time collection of traffic data would be available in a similar domestic case'.
Article 46: Mutual legal assistance in the interception of content data	Cooperate 'to the extent permitted under treaties applicable to them and under their domestic laws'.

Article 40, para 21.

Mutual legal assistance may be refused: (a) If the request is not made in conformity with the provisions of this article; (b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests; (c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction; (d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.

FIGURE 2 Measures covering international cooperation.

Dual criminality

Dual criminality, the principle that both requesting and receiving countries share the same law, is addressed in Chapter V. It does not exist as a general safeguard guiding cooperation across the treaty. In Chapter V, there is an article dedicated to it in the general principles for international cooperation, but this is to make allowances for the fulfilment of dual criminality, and does not make dual criminality a requirement across the chapter, stating 'whenever dual criminality is considered a requirement'. As a requirement for cooperation, it is addressed within certain articles, such as extradition and mutual legal assistance.

Given the risks for this treaty, as outlined above, dual criminality should be a requirement for cooperation across all measures in the international cooperation chapter, including the collection and processing of data for evidence in investigations.

Protection of personal data

Protection of personal data – which is unique to this international criminal justice instrument, given that its focus is criminality associated with technology – is acknowledged in the preamble and addressed in Article 36 of Chapter IV: International cooperation. Much of the language that was being negotiated has been pared down, but the article provides for states to require that data transfers are in compliance with domestic laws and relevant international law, and reiterates there is no requirement to transfer data if this is not in compliance with these laws, saying that states can impose conditions to achieve compliance. It is welcome that domestic law is referenced here as a means to limit cooperation in cases where adequate levels of data protection do not exist in a requesting country. The third clause of Article 36 allows for transfers to third parties, specifically to other states and international organizations. Some states drew a hard line on transfers to third parties, so this may become an issue once the next negotiations begin.

Currently there is ambiguity about how data protections set out in Article 36 can be applied as reservations in the rest of the chapter, and the treaty overall. There is no reference to the provisions on data protection as a requirement for mutual legal assistance. MLATs are the main vehicle by which requests for data collection, preservation and sharing will occur, and not having a direct reference to Article 36 could leave it open to interpretation as to how data protection reservations can be applied and when. Nor is there a reference to it in other articles, such as real-time collection of data (Article 45) or interception of content data (Article 46). There should be a direct reference tying Article 36 to the remainder of the chapter to avoid any confusion on how Article 36 applies in the treaty.

Chapter VII: Technical assistance and information exchange

The technical assistance chapter has been stripped of previous safeguards, which included the principle of transparency, sustainability and accountability. In streamlining the activities from the previous draft, and in line with requests from the African Group, CARICOM and others,[10] these references have been removed, as have the provision of activities that were less law enforcement-focused, such as protection of personal data and privacy and gender mainstreaming. There is also no activity that explicitly focuses on strengthening judicial capabilities and oversight for combating cybercrime – an omission that should be addressed. However, transfer of technology has made it into the draft, which was not advocated for by a large number of countries.

While one may ask why there is a need for safeguards in technical assistance, this is a key method by which the treaty is implemented and given the type of trainings and technologies that may be shared, it is necessary to strengthen this chapter's inclusion of safeguards.

CONCLUSION

With the zero draft, this treaty is poised to set new precedents as the first global cyber-focused legal instrument. Thus far, the process of establishing this treaty has been a tightrope walk, and a balance still needs to be struck between criminalization, potential powers that governments could exercise in implementing the treaty and encoding protections into the provisions of the treaty to safeguard human rights. Much of the language around the scale and scope of criminalization remains ambiguous, and this leaves the treaty exposed to risk in its implementation. There are real risks in leaving measures and actions in this treaty open to wide interpretation.

In the August UN session in New York, states will continue to advocate for their priorities and this is an opportunity to address the challenges outlined in this policy brief and to work towards forging a treaty that counters cybercrime, is bound by international law and criminal justice principles, and, most importantly, does not become a UN-sanctioned tool for state repression using ICT and technology.

NOTES

[1] Fifth intersessional consultation of the Ad Hoc Committee, Vienna, 20 and 21 June 2023, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/5th-intersessional-consultation.html.
[2] Previous positions and analysis can be found here: UN Cyberwatch, GI-TOC, https://globalinitiative.net/initiatives/un-cyberwatch/.
[3] See Summer Walker and Ian Tennant, Spring forward: States to review part II of draft cybercrime treaty, GI-TOC, April 2023, p 9; Summer Walker and Ian Tennant, Wood for the trees, GI-TOC, 2 Feb 2023, https://globalinitiative.net/analysis/international-convention-ict-crime-ahc-un/.
[4] Summer Walker, Still poles apart, GI-TOC, June 2023, p 15, https://globalinitiative.net/analysis/un-cybercrime-treaty-negotiations/.
[5] The article states: Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
(a) The criminal offences established in accordance with articles 6 to 16 of this Convention;
(b) Other criminal offences committed by means of [a computer system] [an information and communications technology device]; and
(c) The collection of evidence in electronic form of any criminal offence.
[6] UN General Assembly, UN Doc. A/AC.291/22, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft Text of the convention, 29 May 2023.
[7] See UN Convention Against Transnational Organized Crime, https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
[8] Nate Schenkkan and Isabel Linzer, Out of sight, not out of reach: The global scale and scope of transnational repression, Freedom House, February 2021, https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.
[9] Rebecca Bellan, 'Teen and mom plead guilty to abortion charges based on Facebook data', Tech Crunch, 1 July 2023.
[10] Fifth session of the Ad Hoc Committee, 11–21 April 2023, Vienna, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main.