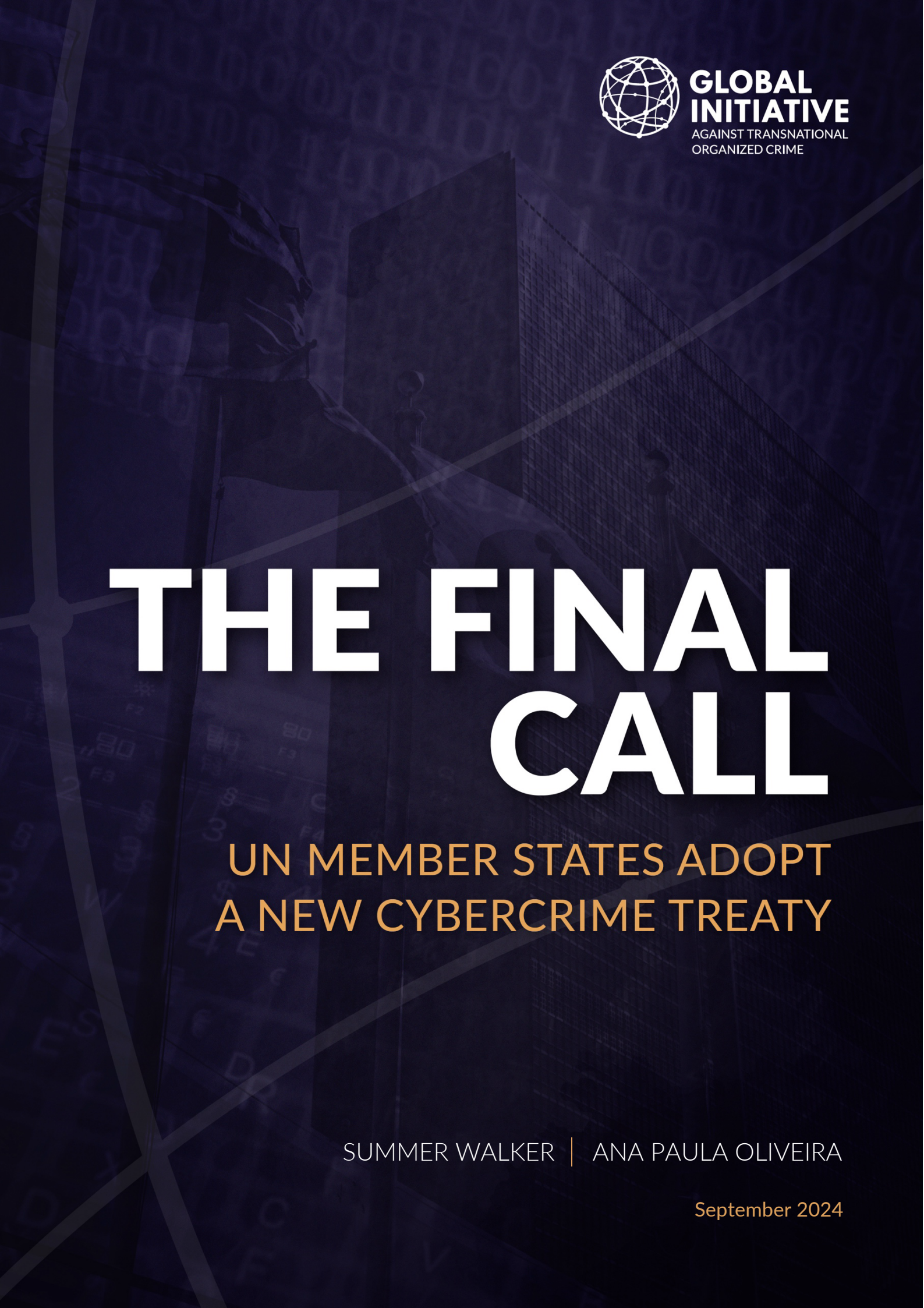

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

THE FINAL CALL

UN MEMBER STATES ADOPT A NEW CYBERCRIME TREATY

SUMMER WALKER | ANA PAULA OLIVEIRA

September 2024

ACKNOWLEDGEMENTS

The authors would like to thank the Global Initiative Against Transnational Organized Crime (GI-TOC)'s multilateral engagement team for regular monitoring and analysis of the cybercrime treaty negotiations. The authors would also like to thank the GI-TOC's Publications and Communications teams.

ABOUT THE AUTHORS

Summer Walker is the GI-TOC's head of security and rights initiatives. She leads projects and provides research and analysis on international policy, with issues ranging from drug policy to cybercrime. She has worked with the United Nations, international NGOs, development agencies and research institutes.

Ana Paula Oliveira is a senior analyst in the GI-TOC's Global Policy team. She provides analysis on a range of policy issues, including the impact of organized crime on human rights law and policy, human rights responses to transnational organized crime, cybercrime and organized crime violence in the context of illicit economies. She has an LL.M. cum laude in international law from the Graduate Institute of International and Development Studies in Geneva.

NOTE

This policy brief was produced with the support of the United Kingdom's Foreign, Commonwealth and Development Office (FCDO). However, the views expressed do not necessarily reflect the UK Government's official policies.

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

www.globalinitiative.net

Contents

SUMMARY **1**

Key takeaways 2

THE GOOD **3**

Respect for human rights 3

Safeguards extended to international cooperation 3

Non-discrimination clause 4

Child sexual abuse material and non-consensual dissemination of intimate images 4

Data protection and gender 5

THE BAD **6**

Scope on crimes too wide 6

Technical assistance is narrow and excludes the wider justice system 6

Collection and interception of data 7

Redefining 'computer system' 7

THE UGLY **8**

Follow-up weak and non-mandatory 8

HOW DID WE GET HERE? **8**

Voting 9

CONCLUSION **11**

Notes 12

SUMMARY

The UN has finalized a treaty on cybercrime, after two years of negotiations. While the governments seemed to feel a sense of closure and accomplishment after years of negotiating this treaty, it did not put most stakeholders at ease with the final text, worrying that it will be misused as a tool by autocratic regimes to access data for political or social repression.

It was the second attempt to finalize the treaty by reaching agreement on the key sticking points that have divided states for over two years on the approach, content and wording of this legal instrument. In the end, Iran called for votes in an unsuccessful bid to have certain items that safeguard human rights removed. All were defeated, and the convention was adopted. The treaty now heads to the 2024 General Assembly for adoption, and can then be ratified by governments.

The ability to collect and share electronic evidence drove the negotiations and shaped core elements of the final treaty. This was the main objective of many countries, who got what they wanted: a wide scope for the collection of data. In the end, it was even written into the subtitle: 'Draft United Nations convention against cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes'.

Electronic evidence collection is allowable for serious crimes (i.e. those punishable by over four years' imprisonment) or 'other criminal offences committed by means of an information and communications technology system' (for which no definition is given). This will allow law enforcement and other government agencies, including intelligence agencies, to trade very easily in electronic data and compel service providers and the UN to cooperate. The articles relating to mutual legal assistance and technical assistance are also focused primarily on collecting, sharing and using electronic evidence. So, while the treaty could be used to build up responses to crippling incidents, such as ransomware attacks, every indication so far is that the focus of implementation will be data collection. This will depend on which countries ratify, who is available to provide support on technical assistance and who drives the limited resources for treaty implementation while the UN is under austerity measures.

Although a cybercrime treaty for the UN is a timely and important undertaking, concerns over its true intent and purpose – as well as the divergent views of governments – hung over the process.[1] And although there are positive aspects in the treaty, such as articles on human rights, data protection and a non-discrimination clause, there are also numerous risks. Like Sergio Leone's classic movie, *The Good, the Bad and the Ugly*, the draft treaty is the culmination of an uneasy alliance among the member states negotiating it. This brief analyzes the positive and negative aspects of this treaty, the first cyber legal framework delivered by the UN, following the process from its onset and through the trajectory of the negotiations. While the treaty confers much cooperative enforcement powers to governments, including the legal right to access e-data, it is worryingly lacking in oversight detail and could present global surveillance threats – as many have warned.

Key takeaways

- Given the wide scope and invasive powers afforded by the treaty, the strongest provision to push back against potential treaty abuse is contained in Article 6: 'Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.' Although many safeguards in the treaty are bound to particular chapters, Article 6 is a provision that encompasses the entire treaty and should be used to frame the application of the treaty by governments and UN agencies in their support for its implementation. Below, this brief assesses the safeguards in more detail.
- Multistakeholder involvement: The Ad Hoc Committee process was widely recognized for its inclusive approach to outside voices – from the private sector to NGOs. However, this good practice was not reflected in the procedures set forth in treaty implementation. For example, the language for a follow-up mechanism to the treaty is weak and non-binding. Some governments' statements during the negotiations and the final text of the treaty seem to want it both ways: they want multinational tech companies to provide technology, equipment and training to carry out the measures afforded by the treaty, but they also want strong powers to compel these companies to do as the governments wish, and they want little oversight over this instrument. It is far less likely that engagement will happen on technical assistance if the ability to monitor and have an impact on treaty norms and policy are lacking. Given the wide-ranging powers afforded by the convention, the weak language around review, oversight and engagement by outside groups, such as civil society, is worrying.
- Optional protocols to the treaty: These were hotly debated, and it was suggested by some that they would be tools to widen the scope on criminalization even further. The final draft allows for protocols but does not designate specific issues that can be covered in them. States opposed to longer lists of crimes in protocols should consider how to use this mechanism and introduce their own protocols as bargaining chips in the process.
- Given that provisions for technical assistance are very narrow, states should use the prevention chapter to design UN agency programming. Often, prevention chapters are filed away and unused, except for at side events alongside annual convenings of states. But given the very technical nature of the assistance chapter, clauses in prevention could be used for judicial training and broader assistance than that listed in the technical assistance chapter.

THE GOOD

Throughout the process, Western states and many Latin American ones advocated for limitations in the scope of the treaty, primarily by restricting the list of crimes included in it, and by including human rights references and legal safeguards, and specific articles on data protection. Canada and New Zealand led the effort to reduce the scope by limiting references to crimes other than those listed in the treaty, but in the end were unable to gather sufficient support to achieve this.

These collective efforts, however, can be seen in places in the wording of the final draft – in particular in the preamble, Article 6, Article 24 and Article 40, paragraph 22. These contain many of the provisions Iran tried to remove, unsuccessfully, from the final draft by vote. There were significant efforts to weaken language on these two topics. That they remained is testament to the efforts of those states that advocated for limits. Though it is not yet known whether these provisions will be sufficient to prevent risk of abuse arising from the treaty, they are a step forward on other existing criminal justice instruments.

Respect for human rights

Under general provisions for the entire treaty, Article 6 underscores respect for human rights as an overarching obligation and serves as guidance on how the treaty should be interpreted.[2] In addition, another layer of protection was inserted in paragraph 2. This is a welcome inclusion that recognizes the specific risks the convention might pose to human rights and serves as a safeguard that governments and civil society will be able to point to when trying to contain any overreach sought through this treaty. The provision stems from a Canadian proposal:[3]

> Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.

Although the inclusion of this article is welcome, the provisions could have been clearer if they had included explicit references to human rights instruments, such as the International Covenant on Civil and Political Rights as a baseline.[4] Moreover, whether such a provision will be respected is not guaranteed and this will require states to be transparent in how they implement the treaty.

Safeguards extended to international cooperation

Article 24 was one of the most hotly debated. The article mandates that state powers and procedures in criminal investigations should be implemented in compliance with international human rights standards. It outlines a number of human rights safeguards and guarantees that state parties should ensure when exercising a state function that can impact on individuals' rights, such as the provision of judicial or independent review, the right for effective remedies in case of abuse, provide justified application of the measure, and that measures or powers are limited in scope and duration. State parties must consider the impact of these powers on third parties, balancing public interest and justice.

One of the key debates was over whether the same conditions and safeguards would apply to both domestic criminal investigations and international cooperation. Article 24 includes a paragraph that mandates states to apply the same conditions and safeguards established at the domestic level to the powers and procedures used for the purpose of rendering international cooperation, thereby extending the scope of safeguards to the sphere of international cooperation.

The wording of this article, however, has shortcomings.[5] There is overemphasis on domestic law, couching the rights afforded within states' domestic frameworks, and not all states may afford these rights. This is problematic because the possible states parties to this convention have widely divergent views on, tolerance for and standards of human rights. For instance, an obligation for exercising judicial or independent oversight is limited by paragraph 5, which states this oversight is only to be applied at the domestic level. The implication therefore is that this relies on the strength of domestic judicial systems and may limit international oversight of arbitrary application of the powers of the convention.

Non-discrimination clauses

There is an important safeguard relating to grounds for refusal of mutual legal assistance included in Article 40, paragraph 22. This safeguard can also be applied to general principles of international cooperation for collecting electronic evidence: 'For the purpose of the collecting, obtaining, preserving and sharing of evidence in electronic form of offences as provided for in paragraph 1 (b) and (c) of this article, the relevant paragraphs of article 40, and articles 41 to 46 of this Convention shall apply.'

This article originated from a provision proposed by New Zealand during the concluding session. In a nutshell, the provision provides states with an opt-out from cooperating on the basis of prohibited grounds for discrimination. Under this article, states may refuse to cooperate if there are substantial grounds for believing that the request by the other state has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions. This is a welcome step towards a more protective framework – especially as the scope remains broad by allowing for cooperation on any serious crime. However, it misses the opportunity to refuse cooperation for political offences, as had been proposed by Costa Rica.

Child sexual abuse material and non-consensual dissemination of intimate images

The inclusion of articles on child sexual abuse material and non-consensual image sharing provides a new tool for governments and stakeholders to prioritize fighting these crimes. However, language on consensual sharing of images by children was a long-debated issue based on moral judgements, leaving provisions weaker than they could have been.

Criminal offences included in the treaty are for the most part cyber-dependent (i.e. those that depend on the use of computer data and online systems). However, the criminalization chapter also includes some cyber-enabled crimes, including offences related to child online abuse material and non-consensual dissemination of intimate images. These two provisions reflect an intent to protect children against crimes committed against them online and the misuse of the internet to commit gender-based violence, for example. Many governments do not address this adequately and it has become a form of crime that is increasingly destructive and widespread. Heightened awareness of and attention to such crimes are welcome, if addressed in a sensitive manner.

The adoption of articles 14 and 16 was not an easy task and they were held up until the end when several paragraphs were called for a vote. Although all member states agreed on the importance of protecting children, how the provisions were to be crafted was more contentious. The debates hinged on including terminology to indicate that only activities with the specific intent to commit a crime are criminalized; avoiding overreach; the need to specify that the material in question must represent a real person or depict child abuse; the possibility of not criminalizing children who create self-generated material; and the need to protect minors from the non-consensual sharing of intimate images.

The amendments and inclusions in these articles were seen as necessary by some states to address child sexual abuse material and non-consensual dissemination of images, while at the same time avoiding the risk of criminalizing children and protecting freedom of expression. They were widely supported by Iceland, UK, Norway, Netherlands, Australia, Japan and others. Other countries, which deemed such provisions as running counter to their values, were vocally opposed to the amendments. As a result, the draft text falls short of making it mandatory for states to exclude the criminalization of children for self-generated materials. The option was to make it non-mandatory by including the formulation 'may take steps …'.

Data protection and gender

The inclusion of and specific language on data protection and gender mainstreaming were long debated. It is an achievement that both are in the convention. Given the lack of consensus, however, the language is not as strong as it could have been. The preamble contains a paragraph that includes 'the right to protection against arbitrary or unlawful interference with one's privacy, and the importance of protecting personal data'. This reference is important, in that it recognizes the risk that governments might arbitrarily interfere in people's privacy through the measures enabled by the treaty. Nevertheless, the provision is couched in weak terms: 'acknowledging the right'. More prescriptive language demanding that states must actively protect such rights would have been preferable.

The same applies to the paragraph in the preamble that 'recognizes the importance of mainstreaming a gender perspective in all relevant efforts to prevent and combat the offences in the treaty'. Although this reflects a recognition of the differentiated impact of crime on gender, the convention falls short of incorporating a broader gendered approach.

THE BAD

Scope on crimes too wide

The scope of crimes that the treaty can be used to address remains wide in the final draft. The draft text provides for cooperation on crimes established under the convention, for serious crimes (i.e. those that are punishable by four years or more) and 'other criminal offences'. The main measures are focused on enabling the collection of electronic evidence, which would be permissible for any criminal offence or serious crime, depending on the context. Other actions, such as extradition, are permissible only for crimes outlined in Chapter II.[6] Governments were broadly in alignment on this wide scope from early on, except for a small number, including Canada and New Zealand. However, private sector actors and civil society voiced concerns throughout the process over the risks posed by the wide-ranging scope of activities that can be criminalized under this treaty.

The criminalization chapter (which lists specific crimes that the treaty aims to address) remains focused primarily on cyber-dependent provisions – an overly broad criminalization chapter could encourage cybercrime laws that criminalize online content. However, protocols may be used in the future to try to expand the scope, as suggested by Russia during negotiations.

Chapter IV: Procedural measures and law enforcement apply to other criminal offences committed by means of an information and communications technology system; and the collection of evidence in electronic form of any criminal offence.

Chapter V: International cooperation allows for collection of e-evidence for any serious crime.

The treaty includes two mechanisms that have the potential to expand its scope even further. One is in Article 4, which imposes on states the obligation to make criminal offences those established in accordance with other United Nations conventions and protocols under domestic law when committed through the use of information and communications technology systems. This provision is a version of earlier articles from previous drafts.[7] The resultant ambiguity of what could then be criminalized will create confusion in implementation.[8]

Technical assistance is narrow and excludes the wider justice system

The chapter on technical assistance (Chapter VII) lays bare the interest of the treaty because it shows where support from the UN will focus to implement it. The technical assistance measures listed are concerned with technical capabilities, mostly directed at law enforcement's ability to track and collect data, evidence and proceeds from cybercrimes or crimes that use an ICT device.

However, there are no measures for legal training or judicial oversight of electronic evidence collection, or how to properly use electronic data in building legal cases, which includes personal data security. These omissions are not only worrying from a rule of law perspective, but beg the question, what would be the point in providing support to request, collect and retain data if such data could become inadmissible in future legal proceedings from improper handling? The two references to legal support are for victim and witness protection, and a vaguely

worded training in relevant procedural law and regulation. This chapter is key because it outlines – and limits – what activities UN agencies will carry out related to this treaty. And unlike the scope in the powers of the treaty, this section is quite narrow.

Throughout the negotiations, the technical assistance provisions were stripped of rights-centred training and gender mainstreaming support. However, as it stands now, the list of provisions does not even include basic judicial support for a criminal justice treaty, let alone training on how to protect data.

Collection and interception of data

Articles 28–30 could have a chilling effect on economies, and in particular multinational companies choosing to store data in other countries outside their headquarters, including tech companies, banks and other sectors. These articles, particularly 29 and 30 (real-time collection of traffic data and interception of content data), include language that 'compels' service providers to turn over data to countries that request it. The language is taken from the Council of Europe's Budapest Convention on Cybercrime, but as has been pointed out,[9] this is a global treaty between countries with very different interests and interpretations of its purpose.

With this wording in this treaty, state authorities would be able to request data from service providers if they believe that 'a range of serious crimes as determined by domestic law' have been committed. And this is not limited to the crimes defined in the treaty. Both articles include a clause allowing governments to pass legislation that would 'oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it' – meaning that service providers would not be able to publicly disclose countries' requests for data. States could use these articles to request data from global banks, tech and social media companies, and others in secrecy if the servers are on their soil. This could create a chilling effect across multiple economic sectors, let alone for criminal justice cooperation.

Redefining 'computer system'

In the use of terms, delegates took the definition of computer system from the Budapest Convention and relabelled it as 'an information communications technology system'. It is not only odd to create inconsistency with existing treaties, but it also muddles terminology and introduces two distinct meanings. ICT is a much broader term that can include radio, television and even satellite technology. The expanded terminology facilitates the inclusion of content-related crimes, which could include social media posts and private messaging through an app. A laundry list of crimes did not make it into the treaty draft directly, but ICT terminology functions as a back door to potentially widen the scope of data that can be collected by governments.

THE UGLY

Follow-up is weak and non-mandatory

The chapter on implementation delivers weak oversight provisions. A review mechanism is not mandatory, nor are inputs from non-governmental stakeholders. The optional quality written into the convention will make it much easier for governments to push back on civil society participation and review of government actions, even when these are carried out in partnership with UN agencies.

Some of the statements by governments during the negotiations and the final text of the treaty seem that they want it both ways. They want multinational tech companies and governments with sophisticated technology to provide technology, equipment and training to carry out the measures afforded by the treaty (most evident in the technical assistance and prevention chapters), but they want strong powers to compel these companies to do as the governments wish, and they want little oversight over this mechanism that will create these new possibilities. It is far less likely that engagement will happen on technical assistance if the ability to monitor and have an impact on treaty norms and policy is lacking.

Given the vast powers afforded by the convention, the weak language around review, oversight and engagement by outside groups is worrying.

HOW DID WE GET HERE?

The basis for discussion was the third revised draft text of the convention published by the Ad Hoc Committee ahead of the final session.[10] Under the Chair's guidance, member states dedicated the first week to discussing the changes in the draft text. The idea is that this would allow member states to enter week two with a final document to adopt in plenary by consensus or vote.[11]

Deliberations reflected the same issues from previous sessions: whether the balance between human rights and state powers was appropriate, particularly in articles 24, 35 and 40; divergent views on the convention's title, which for many would confuse the terminology between cybercrime and information and communications technology; and lack of consensus on a key article on child sexual abuse material and exploitation. The interventions revealed a continued lack of a shared vision for the treaty.

As the session progressed, other key issues remained unresolved. One was the potential for this convention to include additional crimes beyond those listed in the final draft in the form of supplementary protocols, as mentioned above.[12] States were divided on this idea, which, like the convention itself, was proposed by Russia. There was some support for the protocols, but other states would prefer to postpone this discussion and focus on ratifying and implementing the main convention before considering additional protocols. Some states, including Ecuador, Liechtenstein, South Africa and Vanuatu, argued that discussing protocols one year after the convention enters into force (the timeframe proposed by the Chair) would be premature and that not all countries would have the resources to enter into negotiations on a convention that has not yet been implemented.

The other was the threshold for ratification for the Convention, which became somewhat connected with the protocols discussion. Mexico proposed increasing the threshold of ratifications for the convention to enter into force to 60 countries, meaning more member states would be party to the treaty when it enters into force, with greater likelihood of the convention garnering wider agreement. This became a way of engineering a larger number of participants at the Conference of Parties that would approve the protocols and allow more time for identifying gaps and the actual need for a protocol.

Outside the meeting room, the human rights risks posed by the treaty and warnings from civil society and the private sector attracted press attention. The negotiations even featured in the UN Secretary-General's daily press briefing.[13] When asked about the Secretary-General's position on a possible UN treaty that could increase human rights abuses, his spokesperson said: 'We very much hope that member states will find consensus, and as with any treaty, in a way that continues to guarantee all of human rights contained in the Universal Declaration of Human Rights.'[14] During a briefing, participants acknowledged the Chair's openness to multistakeholder participation but also expressed fundamental concerns about the current draft. Many have voiced that the guidance offered by the Office of the UN High Commissioner for Human Rights to the Ad Hoc Committee[15] should be the minimum basis for a functioning treaty in terms of its human rights perspective – something that is certain to meet with resistance from a number of member states.

Following informal discussions, the Chair presented a new proposal on provisions related to human rights and safeguards, on supplementary protocols, scope, offences related to child sexual abuse material and on the title of the convention. States were left with very little time to make final bargains and pleas before adopting the draft by consensus.

Voting

In the final hours of the meeting, Iran raised several objections to the draft and took them to a vote among member states. Iran asked for a vote on articles 6.2 (on human rights); 14, paragraphs 1 and 3; 16, paragraph 1 (offences related to child sexual abuse material); 24 (conditions and safeguards) and 40.22 (grounds for refusal). In all of the cases on which they took issue, Iran fell far short of the two-thirds majority needed for their proposals to be accepted (see below). In the case of one vote, Iran was backed by the Democratic Republic of the Congo; other than that, they were the only government to raise objections during the session on the final text of the treaty.

Once this process had wrapped up, the Chair asked the committee to adopt the convention by consensus. No objections were raised.

Vote called by Iran to delete Article 6, paragraph 2 (related to human rights)

In favour **23**
Against **102**
Abstentions **26**

Vote called by Iran to delete wording 'without right' from Article 14, paragraph 1 (related to online child sexual abuse or sexual exploitation material).

In favour **44**
Against **98**
Abstentions **11**

Vote called by Iran and DRC to delete Article 14, paragraph 3 (related to online child sexual abuse or sexual exploitation material).

In favour **51**
Against **94**
Abstentions **10**

Vote called by Iran to delete 'and without right' from Article 16, paragraph 1 (related to non-consensual sharing of intimate images).

In favour **38**
Against **99**
Abstentions **13**

Vote called by Iran to delete Article 16, paragraph 3 (related to non-consensual sharing of intimate images).

In favour **34**
Against **99**
Abstentions **19**

Vote to delete Article 24 (related to conditions and safeguards)

In favour **10**
Against **110**
Abstentions **30**

Vote called by Iran to delete Article 40, paragraph 22 (related to grounds for refusal of mutual legal assistance)

In favour **25**
Against **109**
Abstentions **17**

Following the vote, some delegations expressed optimism about the convention and the potential for international cooperation to combat cybercrime; others expressed reservations and concerns about certain articles, particularly those related to the protection of children (Niger, Djibouti, Pakistan, Papua New Guinea, Vietnam, Iraq, Guatemala and Mali) and human rights (Malaysia, Mali, Iraq and Vietnam), as well as the title of the convention (Russia and Cuba).

CONCLUSION

The text will now be submitted to the UN General Assembly for formal adoption. Once adopted, states will start domestic processes to ratify the treaty. According to article 64, the treaty enters into force on the 90th day after the 40th member state deposits its ratification, acceptance, approval or accession to the treaty. However, there is no timeline for member states to do that and the process for states to agree with the treaty internally will now mainly depend on parliaments and countries' domestic systems to consent to be bound by international instruments. Treaty implementation will therefore depend on the legislative branches of many jurisdictions. This, of course, can delay the process for the treaty to enter into force.

Considering how the process was pushed forward to bring it to a conclusion and how many countries reiterated a need for the treaty, especially those seeking technical assistance, it is likely to be ratified by 40 member states. The question remains whether those countries that store the data and have the technology will accede to the treaty quickly enough to enable the international cooperation and assistance many hoped to achieve with this instrument.

Considering the broad scope of the treaty, the possibility of expanding crimes under it and the possibility for reservations, a human rights-based approach to monitoring and implementing the treaty will be of paramount importance to avoid misuse and abuse, outweighing the good over the bad of what the treaty might become.

Notes

[1] Summer Walker and Ian Tennant, Control, alt, or delete? The UN cybercrime debate enters a new phase, GI-TOC, December 2021, https://globalinitiative.net/analysis/un-cybercrime-debate/.
[2] Article 6, paragraph 1, Draft United Nations convention against cybercrime, https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf.
[3] Proposal by Canada on behalf of a group of 66 States and the European Union to the Ad Hoc Committee on Cybercrime (AHC) to further define the scope of the draft Convention, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Canada_3.3_05.02.2024.pdf.
[4] GI-TOC, UN and Organized Crime podcast, 'Cybercrime: safeguards matter' episode, https://globalinitiative.net/analysis/un-crime-podcast/#podcast-30682-2.
[5] Ana Paula Oliveira and Summer Walker, Hitting pause: The unfinished story of the UN cybercrime negotiations, GI-TOC, March 2024, https://globalinitiative.net/analysis/un-cybercrime-negotiations-pause/.
[6] Illegal access (Article 7); Illegal interception (Article 8); Interference with electronic data (Article 9); Interference with an information and communications technology system (Article 10); Misuse of devices (Article 11); Information and communications technology system-related forgery (Article 12); Information and communications technology system-related theft or fraud (Article 13); Offences related to online child sexual abuse or child sexual exploitation material (Article 14); Solicitation or grooming for the purpose of committing a sexual offence against a child (Article 15); and non-consensual dissemination of intimate images (Article 16).
[7] Article 17 of the zero draft of the United Nations Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes and Article 60 of the further revised draft text of the convention.
[8] Summer Walker, Closing pandora's box: UN cybercrime treaty negotiations, GI-TOC, August 2023, https://globalinitiative.net/analysis/un-cybercrime-treaty-negotiations-august-2023/.
[9] Summer Walker and Ian Tennant, Control, alt, or delete? The UN cybercrime debate enters a new phase, GI-TOC, December 2021, https://globalinitiative.net/analysis/un-cybercrime-debate/.
[10] A/AC.291/22/Rev.3, Updated draft text of the convention, 23 May 2024, https://documents.un.org/doc/undoc/gen/v24/036/33/pdf/v2403633.pdf.
[11] See GI-TOC, Cyber Convention Check-in: Reconvened session, GI-TOC, July–August 2024, https://globalinitiative.net/announcements/cyber-convention-check-in-reconvened-session/.
[12] Ian Tennant, What's the protocol on protocols? The risks of a last-minute cybercrime treaty protocol, GI-TOC, July 2024, https://globalinitiative.net/analysis/risks-last-minute-un-cybercrime-treaty-protocol/.
[13] See Daily press briefing by the Office of the Spokesperson for the Secretary-General, UN, July 2024, https://press.un.org/en/2024/db240729.doc.htm.
[14] Ibid.
[15] Office of the United Nations High Commissioner for Human Rights, Written submission to the reconvened concluding session of the AHC, 22 July 2024, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/OHRC_AHC_Cybercrime_-_reconvened_concluding_session.pdf.