POLICY BRIEF

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

STILL POLES APART

UN CYBERCRIME TREATY NEGOTIATIONS

Summer Walker

JUNE 2023

ACKNOWLEDGEMENTS

This report was made possible with generous core support from the Government of Norway. Thank you to Ana Paula Oliveira and Darren Brookbanks for their review of the research and to Ian Tennant and Mark Shaw for their thoughtful input.

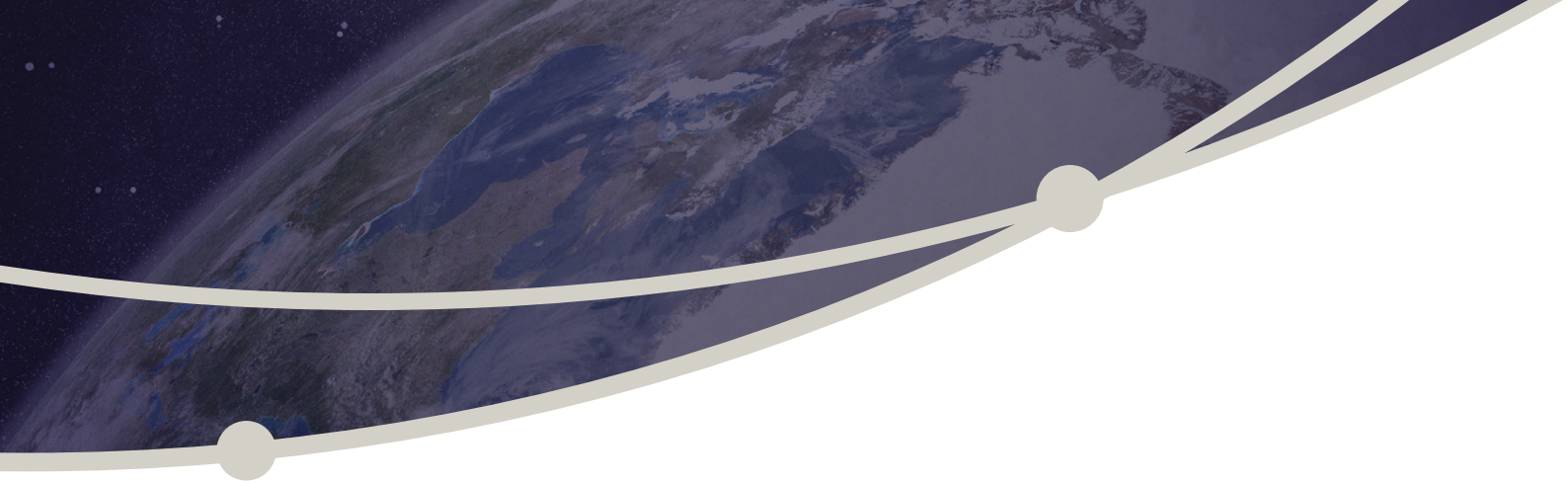
ABOUT THE AUTHOR

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: © *Planet Observer/Universal Images Group via Getty Images*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

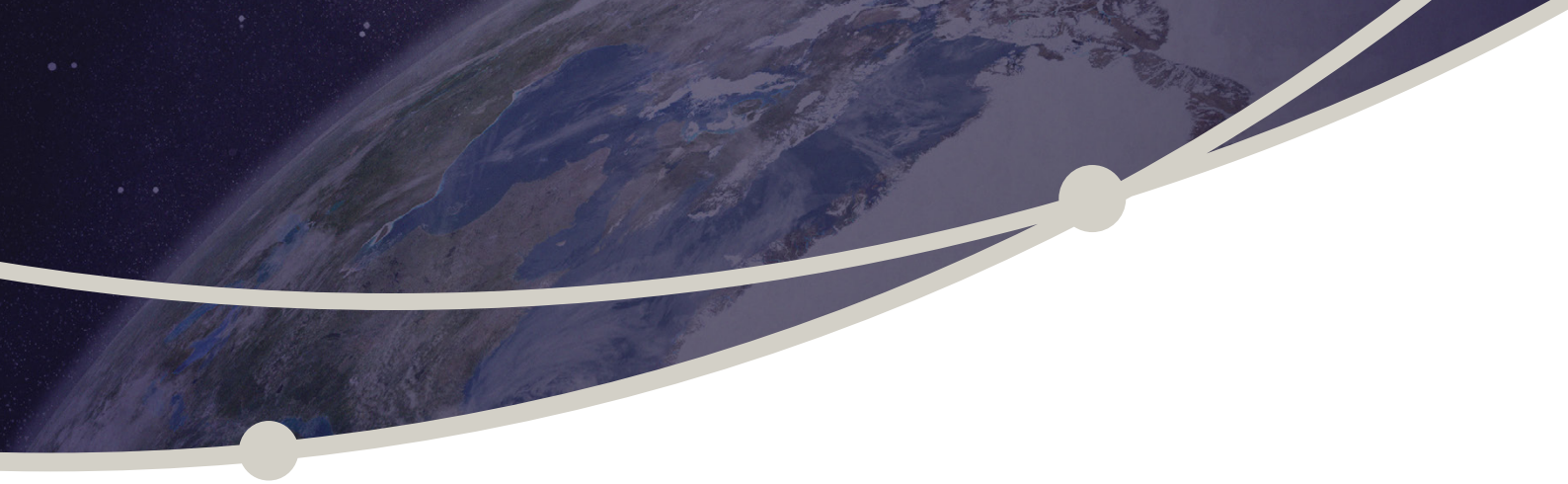
CONTENTS



SUMMARY

The UN Ad Hoc Committee negotiating a treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes (henceforth 'AHC') has completed its deliberations on a negotiating text before a zero draft treaty will be provided to states in June 2023. In January the AHC covered proposed chapters on criminalization, procedural measures and law enforcement, and general provisions. The most recent session, in April, reviewed the proposed chapters on international cooperation, technical assistance, prevention, implementation mechanism, final provisions and the preamble. States and multi-stakeholders will now look ahead to debating a full zero draft at the next meeting in August 2023.

This brief analyzes the state of the negotiation process. It focuses on the fifth session, which ended in April 2023, with specific attention given to the chapters on international cooperation and technical assistance, which are seen by many member states as the key aims of the future convention. It also provides an overview from the January meeting, where criminalization and procedural measures were addressed, focusing on the areas where the widest divergence was seen. The negotiations have been extremely detailed, resulting in a lengthy draft, so not all issues are summarized here. This brief outlines the types of negotiating groupings that governments have divided into, demonstrates how this plays out in negotiations and shows some of the underlying and overt areas of disagreement that will have to be somehow bridged in the August meeting. That meeting is meant to be the last in-person negotiation of the zero draft before a final draft treaty is adopted in early January 2024, so this is a critical moment to look at where the process is.



DIVIDED WE VOTE

Following the April meeting, states are still no closer to agreeing on the convention's key points. Therefore, in August delegates are likely to make decisions on some of the key issues. This even includes terminology to be used. For instance, the choice between using 'cybercrime' versus 'use of information and communications technologies for criminal purposes' has not been made yet.[1] Other topics include the scope of crimes to be criminalized; the scope of international cooperation under the treaty; and whether safeguards around human rights and data protection will be incorporated, and to what extent. The August meeting could be the moment when decisions are taken to a vote if consensus still cannot be reached at that stage.

As has been seen since the early meetings,[2] states are broadly grouped into two opposing poles or camps on the issues of scope of cooperation, and legal and human rights safeguards. And during the April session this pattern continued, with the two groups on either end of the spectrum espousing two very different visions for this future treaty. The first group, which includes several key regional blocs (the African Group, CARICOM (the Caribbean Community) and the Arab Group), wants a broad range of activity with limited-to-no guardrails restricting this. This camp argues that specific language on safeguards, privacy rights and human rights will constrain the treaty's efficiency. The second group, primarily Western European and Others Group states, and Budapest Convention[3] member states – such as Japan, the Philippines, Chile, Czechia, Slovenia and Slovakia – have called for a limited scope of activities to be criminalized and for adequate safeguards on the treaty's application. These states claim safeguards will strengthen the prospects for cooperation, although early on in negotiations they also took a liberal stance on allowing the cooperation provisions to be applied to a wider scope of crimes than those criminalized under the treaty. Then there are states that do not fall into either pole but who align with elements of each, seeking wide cooperation but simultaneously supporting safeguards for human rights, for example. These perspectives are demonstrated in country positions in the text of the treaty and form the basis of many major disagreements in the negotiations.

Thus far, the AHC meetings have, aside from tough exchanges on the Ukraine war, maintained a constructive approach, despite disagreements on substance. But how will states tackle these differences once the zero draft has been completed and they need to make decisions? This is how it may pan out.

Under the rules of the AHC, states are able to take decisions by vote, though they seek to negotiate by consensus and, technically, voting should not happen until efforts to reach consensus have been exhausted.[4] Decisions by vote must achieve two-thirds majority, so a simple majority negotiating

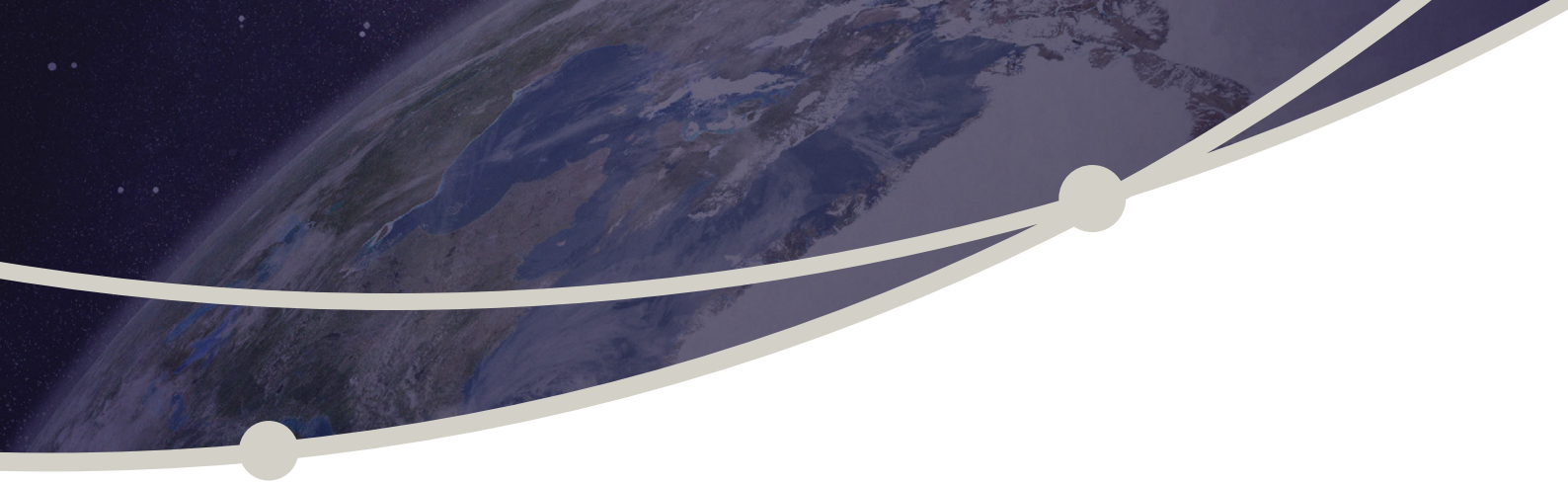
strategy will not work. States with divergent positions will have to make a strong effort to make their case or bring down their expectations to arrive at two-thirds.

One chapter of the draft treaty that could provide incentives for compromise is technical assistance and the funding needed to achieve it. Both of the two main groups have powerful, technologically advanced states that can offer both funding and knowledge for technical assistance, such as China on one side and the United States on the other. How this might play out is unclear but the section below on technical assistance shows that a number of states feel this is their key priority, so leverage in this chapter could become important.

Efforts to bridge divisions between the opposing poles will be needed. States seeking a permissive treaty have already staked positions as far to their side as possible, and received some compromise from the other group, such as on scope of crimes for which electronic evidence can be collected. This may give them leverage once the draft is completed, as finding middle ground could lean in their favour. For the other group, dispelling the false dichotomy between a narrow focus with safeguards and efficiency in implementation should be a key priority through outreach and in negotiations.

In the end, voting may be the tool that tempers positions that are camped on opposite ends of the spectrum. Yet there is still a risk that, out of this, two competing treaties may emerge for international cybercrime cooperation: a wide-ranging, permissive treaty administered by the UN for one group of countries, and the Budapest Convention used as the mechanism for the others.

View of the 11th meeting of the first session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. *© UN Photo/Manuel Elías*



POLE POSITIONS

Cooperate first, question later states

Broadly, this group is seeking to extract as much as possible in terms of enhanced cooperation, procedural capabilities and technical assistance. At the same time many of these countries have been opposed to the inclusion of human rights and legal safeguards, including those related to due process, data protection and references to human rights obligations (such as the right to privacy). Many argue that these would limit the opportunities for cooperation and the efficiency – or expediency – of the convention. In general, this group includes Russia, China, Iran, Singapore, India, the African Group, CARICOM and the Arab Group.[5]

For some of these states, this debate is framed by opposing views among the world's governments on an open internet and digital rights, and the inherent challenges in trying to accommodate those fundamental differences within this treaty. Some governments plainly do not agree with the concept of an open internet that is not under state supervision or control, and this position is most clearly set out in the statements and negotiating positions of Russia, China and Iran.

Other states in this broad group are not taking a stance on open internet principles but are seeking expediency. They are not opposed to some principles of digital rights and open access, but at this stage in the treaty negotiations are putting these aside in search of expansive powers and the improved operational capability that can be achieved through this convention. They seek the widest options available to increase their cross-border cooperation and to improve domestic tech capabilities that are lacking. For many, technical assistance is the most important section of the draft, as is the part dealing with enhanced investigative capabilities. On technical assistance, the African Group has been outspoken about removing wording they think would bind them to conditions on accessing assistance, including language around transparency and accountability. CARICOM has echoed this position, and it is also reflected in Brazil's positions.

Some countries negotiating against safeguard provisions have used the UNTOC and UNCAC as justification, saying they are not opposed to human rights and data protection, but that these two predecessor conventions hardly refer to human rights. Egypt and Iran have been particularly strong proponents of this position. For instance, Tanzania drew attention to this regarding a minimum penalty threshold for extradition. This tactic is often used when language derives from the Budapest

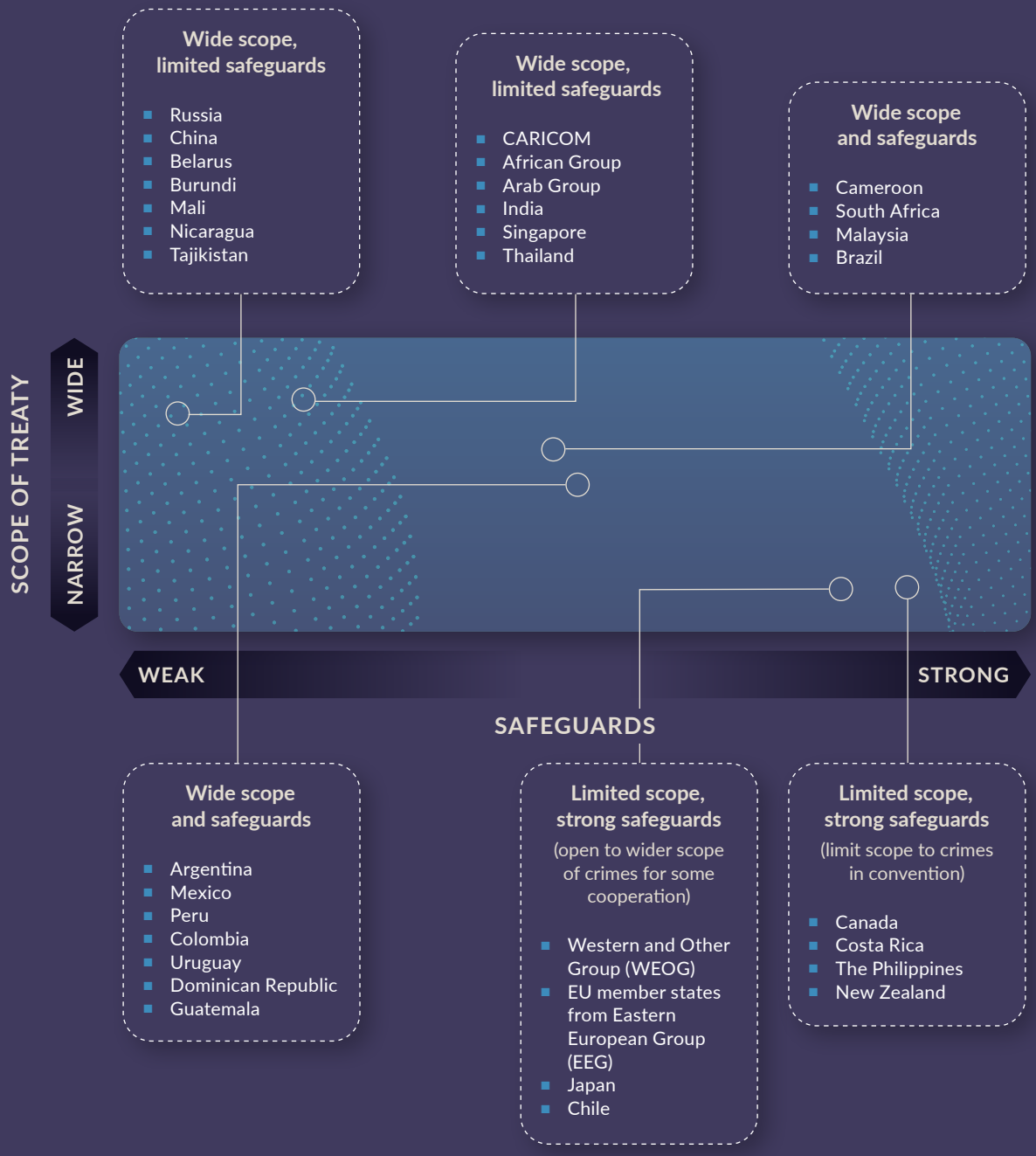


FIGURE 1 On a spectrum: States' positions in the draft treaty.

Convention rather than UNTOC and UNCAC. Although the two UN treaties have informed some of the language used in this draft, they were drafted over 20 years ago, in more trusting and optimistic times for multilateralism, and those are not cybercrime-focused treaties. As can be seen below, relying on language used in these older conventions can raise specific concerns in this new context. A cybercrime treaty is a particularly delicate international instrument in terms of rights and responsibilities, and therefore has to be formulated from a unique perspective, rather than by replicating earlier conventions.

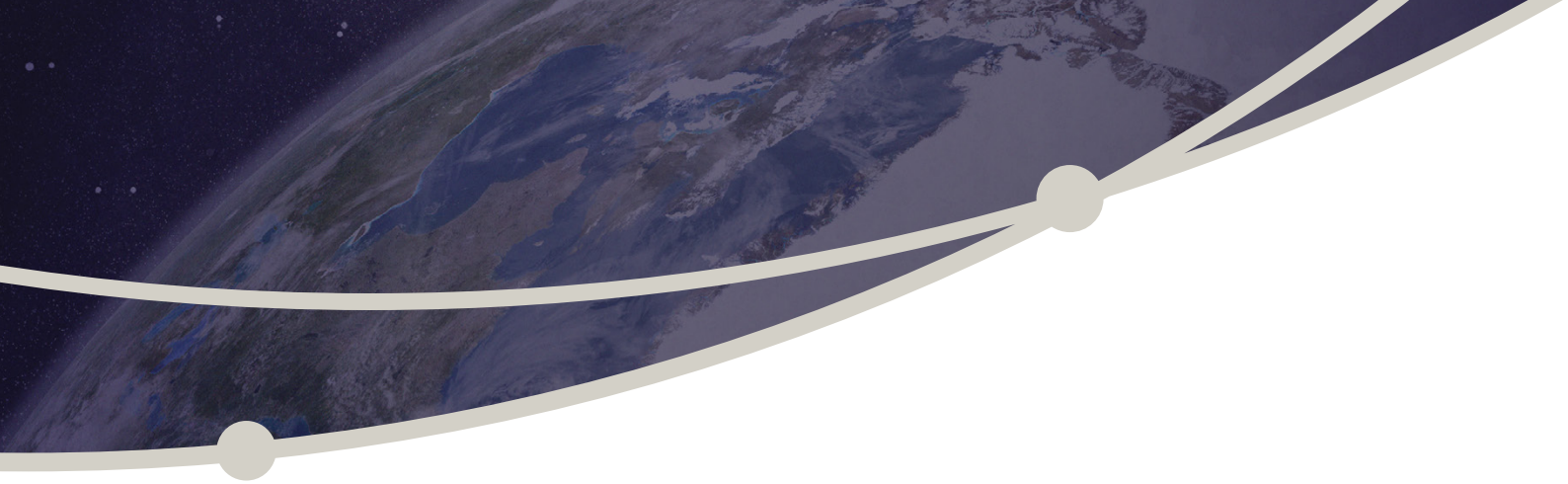
The safeguard states

At the other end of the spectrum is a group of states that have been vocal about the need to limit the powers that will be conferred in this convention through safeguards that are in line with states' human rights obligations, including digital rights, data privacy and procedural rights, and which are designed to protect people from political persecution. They have varying perspectives on data protection clauses and scope of cooperation, such as the range of applicable crimes for collecting e-evidence, but all call for strong safeguards to be included. This group includes the EU countries, Chile, UK, US, Switzerland, Canada, South Korea, Japan, Australia, New Zealand, Norway, the Philippines, Ecuador, Uruguay and Georgia, among others. There are others who are negotiating for a wider scope, but are not opposed to including safeguards, such as Colombia, Uruguay and Peru.

This group also reflects regional and country-level perspectives on issues such as an open internet and digital rights. For instance, the EU is known to have the strongest set of data privacy regulations (embodied in its General Data Protection Regulation), and has emphasized how a convention must not override their standards if they are to accede. In general, on the issue of rights and safeguards, this group has encompassed countries that are largely already able to cooperate with one another under existing mechanisms, such as the Budapest Convention, as members and observer countries.

However, some differences within this otherwise broadly homogeneous group are evident. On scope, the group in favour of safeguards had given ground on the extent of cooperation at the fourth session in January, by agreeing that broader cooperation on some measures could be granted through the treaty alongside a narrow scope of criminalized activities. However, at the fifth session in April a small group of countries emerged as vocal supporters to limit cooperation, arguing that it is an issue of over-stretching capacity for day-to-day cooperation if a treaty were agreed upon (see 'international cooperation' below).

There are also disagreements on data protection in the treaty. In particular, the US and the EU are not aligned on data protection details. The EU's proposals are based on its own high levels of protection provided for in EU regulations, while the US has never adopted this level of privacy safeguards. The US sees the EU's data protection proposals as unworkable under the American criminal justice system, particularly on retaining data on criminal proceedings for the purposes of future appeal hearings. At the same time, others, such as Australia and the UK, voiced more nuanced concern over the EU proposals, stating that this should not be a data protection treaty, as this would be difficult to agree upon.



THE FIFTH SESSION

International cooperation

Regarding the international cooperation chapter, ongoing debates are both technical and overarching. Technical language choices, which will have major implications for scope, continue, as do debates over how expansive (and invasive) cooperation should be.

In terms of language, states continued to debate whether cooperation should encompass 'information and communications technology' and 'information' rather than 'computer systems' and 'computer data'. The former is favoured by those seeking an expansive treaty, whereas the language of the latter seeks to limit the scope of cooperation. Using 'information' rather than 'computer data' is a tactic to cast a much wider net on what can be criminalized under this treaty, advancing an agenda that certain information itself can be illegal.

A disagreement on safeguards continued to present itself. Some states advocated for the removal of references in this chapter to Article 42, the chapeau article on safeguards as it currently stands in this treaty. These included Malaysia, CARICOM, the African Group and the US. Some argued that Article 42 applies across chapters, so does not need to be referred to. The issue is that this is not actually clear in the draft, since this article sits in a particular chapter – Chapter III: Procedural measures and law enforcement – with draft language that only applies to the measures in that chapter.

On the scope of sharing electronic evidence, a small group of countries within the 'safeguards States' group emerged as vocal supporters of limiting cooperation, including cooperation on collection of electronic evidence to crimes listed in this convention (narrow scope). These included Canada, Costa Rica, Guatemala, New Zealand, the Philippines and Peru. Some argued that from a practical standpoint a wide scope will inhibit cooperation, possibly making the treaty unworkable. Canada and Italy, for instance, raised the concerns over capacity challenges in implementation for a treaty that covers 'all crimes' or 'all serious crimes'. Canada said the bulk of requests they receive are for data for an undefined range of crimes, and they spend resources dealing with these requests, including explaining to partner countries how to meet their threshold for data sharing. Canada argued that if the treaty has a wide scope, it would be difficult to implement in reality and could impede concluding the convention. Italy likewise noted cooperation for all crimes committed using ICT would cause budgetary constraints.

Indian police recover SIM cards and other items in a crackdown on a call centre syndicate running a scam.
© Sonu Mehta/Hindustan Times via Getty Images

A number of other countries continued to voice support for a wider scope on cooperation for collecting e-evidence, such as crimes in the convention and serious crimes, including the EU, US, China, Mexico, Nigeria, Norway and Switzerland. The African Group did not take a firm position on the scope of crimes for collection of e-evidence, yet called for the widest measure of mutual legal assistance for collecting e-evidence for investigations and prosecutions.

The middle ground among the three choices for scope of crimes seems to be crimes included in the convention and serious crimes, which also arose in the context of mutual legal assistance. The issue here is, how does one define serious crimes? Mexico suggested using the definition of serious crime from UNTOC: '"Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious Penalty'. The EU also voiced openness to wider cooperation, saying it would have to have a clear threshold, and also setting out punishment by four years (inspired by UNTOC). The UK voiced the need to think carefully about the implications of this chapter, saying that it is open to the convention being used for sharing of e-evidence more widely, but only if robust human rights provisions were in place, which is a different approach from a time-bound requirement.

Using a time-based approach, which has been used in previous treaties, warrants further consideration, as it would still allow for a very wide scope of cooperation. This is also a relevant question for extradition articles. The *Bangkok Post* reports that 69 countries prohibit homosexuality and in 11 countries it is punishable by death.[6] A convention with this definition could allow for data sharing to be used to persecute, imprison and put to death people for their sexual preference by using their online data if punishment in that country for such an 'offence' is at least four years. Clearly, this risk also includes political and social persecution carried out through other laws, such as counter-terrorism measures,

national security and even existing cyber-laws. The death penalty is applied in some countries for offences such as drug trafficking, whereas in others certain drugs have legal markets. Allowing this convention to establish a norm through the UN by which cyber-cooperation allows for cultural, social and political persecution is therefore a real risk.

A clause on protection of data (Article 57), which is very specific to this type of criminal justice treaty, was debated. Singapore and the CARICOM group asked to remove it. The EU set a high bar, saying that the articles will need to respect the EU Charter of Fundamental Rights and data protection regulations as a condition of it acceding to the treaty, suggesting using language in the recent Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Argentina voiced concern over its ability to comply with some of the requirements, while Ecuador supported strengthening the principles of Article 57.

Technical assistance

All states support the inclusion of technical assistance in the treaty and recognize that there are large differences in terms of the capacity of countries to combat cybercrimes. For some states, this is the key chapter and they want it listed as one of the objectives of the treaty, as stated by the African Group in the plenary. This group seeking technical assistance through the treaty includes a wide range of Global South countries that do not align across issues. They call for tailor-made (in the case of the African Group) or beneficiary-driven technical assistance. Many agree on increasing types of technical assistance, but do not align on other issues, such as human rights and gender mainstreaming training, removing language on transparency, or the inclusion of civil society and relevant stakeholders in the process. Another main objective was to request removal of language they thought could hinder access to assistance, which was led by the African Group and CARICOM primarily.

Costa Rica's government has faced crippling cyber attacks. Here an accountant is compelled to sort inventory manually to complete a tax declaration. *© Ezequiel Becerra/AFP via Getty Images*

There was limited support for adding a reference to technology transfer in technical assistance. For instance, Pakistan suggested adding that technical assistance may include transfer of equipment, surveillance and other material support, with special focus on developing countries in Article 86.[7] Other supporters of including technology transfer in the chapter included Iran, Ecuador, Dominican Republic, Venezuela and China (a likely provider of support). Others, such as Thailand, Uruguay and Costa Rica, supported adding a reference to providing 'financial support' in addition to material support.

For many states who would most likely be funders or providers of technical assistance found the general principles for the chapter too vague, and requested clearer, more focused language. These governments also want it made clear that the treaty should reflect the voluntary nature of assistance and does not place any mandatory responsibilities on providers of such assistance. The US in particular said it would not support a UN-funded mechanism, calling for a more flexible approach for donors and recipients. Australia suggested taking from agreed-upon language for capacity building principles developed by the UN Open-ended Working Group on security of and in the use of information and communications technologies, and many states supported this idea. Many in this camp do not support the request to include technology transfer, including the UK, Canada, Japan, Norway, Sweden and the US. Here, China is a major exception and expressed support for transfer of technology where possible.

Transparency and accountability

There were clear dividing lines over the inclusion of references to transparency and accountability. These are currently spelled out in the guiding principles (Article 86), which call for an approach that 'ensures sustainability, transparency and accountability', and in Article 89, which calls for state parties to provide and receive assistance while giving due consideration to the 'principles of shared responsibility, ownership, sustainability, transparency and accountability', and ensuring that assistance is 'subject to appropriate and transparent monitoring and evaluation processes to assess their effectiveness (89.10)'.[8]

The countries in support of these articles should have the upper hand in negotiations because they are already in the text, meaning there will have to be compelling arguments to remove them. Many potential donor countries from the WEOG and Budapest groups voiced support for retaining these points.[9]

In its statement, the African Group questioned whether references to transparency and accountability would create obstacles to assistance in practice. In country statements, some African states took different positions. For instance, South Africa supported Article 89, which includes several references that are questioned by other members of the African Group. Cameroon, in its country statement, echoed support for transparency and accountability. Jamaica, speaking on behalf of CARICOM, noted the full text of Article 89 para 2 is too prescriptive, which includes principles of national ownership and sustainability. CARICOM also wanted to remove 89.10, calling for monitoring and evaluating of technical assistance as a potential obstacle to receiving it.

Partnerships for technical assistance

Included in this chapter are references to who would help support technical assistance besides states themselves. Listed are 'relevant stakeholders (main stakeholders), UNODC, civil society, the private sector, other international and regional organizations, and relevant experts'. There was general support for the inclusion of multi-stakeholders, with some recommendations to adjust the references and streamline the terminology used. It was requested to remove the term 'relevant stakeholders' from the guiding principles, as it gave the impression that relevant stakeholders could receive technical assistance, which is for states.

While no countries questioned the relevance of the UNODC in providing technical assistance, some, including Japan, Colombia and Sweden, questioned the need to establish its pre-eminence in this chapter. For instance, Japan, Colombia and France questioned paragraph 9, which 'entrusts' the UNODC with coordinating and providing technical assistance, saying the language goes beyond previous conventions and that a coordinating role is outside the UNODC's mandate. Some, including Indonesia and the UK, noted that the UNODC is mentioned several times, and that only one reference is needed. Others, including Pakistan and Iran, called for the inclusion of INTERPOL, which is not there currently.

Preventive measures

In this chapter there was a general call for streamlining content. A number of states also noted that some references on financial proceeds of crime and other details are taken from the UNCAC and do not have a clear role in this text. The UK proposed merging lengthy Articles 90 to 93 into a general principles section on prevention, which a number of governments supported or voiced an interest in considering. The Netherlands proposed adding a prevention measure to work with potential offenders to steer them towards lawful pursuits, which many countries voiced support for.

In January 2023, the US Justice Department announced that the FBI had seized the website of Hive, a ransomware group. © *Kevin Dietsch/Getty Images*

China and Russia focused on the need to include obligations and responsibilities of service providers, including placing requirements on them. They suggested including new language on adopting legislation that would require reporting to authorities, and that service providers adopt technology measures to monitor and record network operation status and retain related information for no less than six months. Russia doubled down on China's proposal, supporting it and saying that standards for the private sector are needed along with penalization if standards are not followed.[10] The proposal was largely ignored by most other delegates. Only a couple supported this addition, such as Eritrea, while Australia and New Zealand opposed it and Singapore said applying obligations on the private sector would be untenable.

Implementation mechanism

There is some irony in the fact that states have formed the most consensus around how a treaty that lacks consensus should be implemented. This was largely due to a working group led by the Swiss ambassador in Vienna and the Nigerian vice chair of the AHC to try to forge agreement across the three options laid out in the negotiating document.

The resulting outline consists of applying the UNTOC and UNCAC-style Conference of Parties to this treaty with the UNODC as the secretariat. This was preferred to the two other options presented – placing the Conferences under the UN Commission on Crime Prevention and Criminal Justice (CCPCJ) (as proposed by the US) and a second, which included a permanent international technical commission partially led by the International Telecommunications Union (as proposed by Russia). In presenting the new option, the co-facilitators clarified that they did not find broad support for options two and three, but identified pieces of each proposal that some states were interested in bringing into the new option.

Those supportive of option one (the Conference of Parties approach) felt it would allow for inclusivity of member states that ratify the treaty and that it is a tested model that works. It was also noted that improvements could be made, including a number of states for whom inclusivity for multi-stakeholders is key, and prefer the working methods of the AHC itself for this. The new proposed mechanism maintains the option for subsidiary bodies such as working groups without baking in a permanent commission.

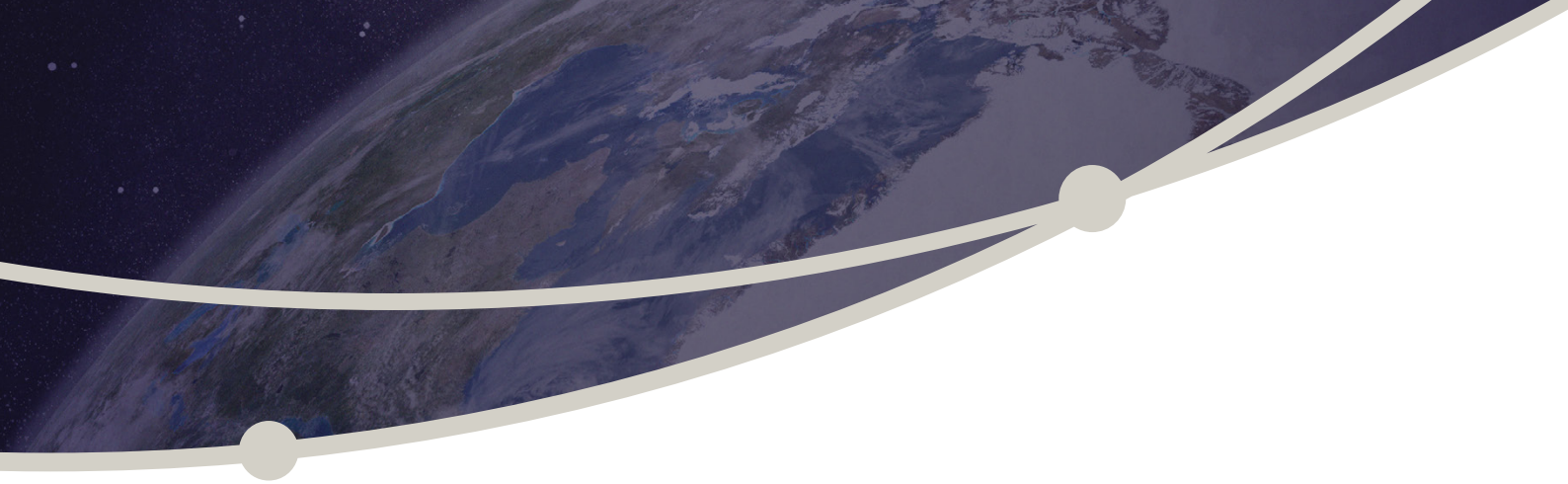
While it contains references to cooperation with relevant stakeholders, it does not lay down any rules for operation, leaving that to a future Conference of Parties to decide on. Nor does it explicitly reference a review mechanism but includes the types of information that should be shared, including lessons learned and efforts made to implement the convention. With regard to the more difficult elements on civil society access, funding and detailed modalities, states seem in favour of negotiating this later, opening up risks to the delays and restricted civil society access of the kind seen in the UNTOC and UNCAC models.

Preamble

As CARICOM pointed out, the preamble can be used as a tool to interpret the convention, so its final contents are paramount. At the same time, a number of governments, including South Africa, Canada and Australia, expressed that it was too early in the process to hammer out the details of the preamble until it is known what the chapters of the convention will finally hold. For instance, there are multiple ways crimes are referenced in the preamble, which will be resolved – hopefully – once states choose the terminology for the rest of the convention. There were also calls from China, the US and the UK, and others to streamline this section more generally. Similar patterns played out, with calls to remove references to human rights and data protection from one side of the spectrum and calls for their inclusion from the other.

Final provisions

On final provisions, there was disagreement on how many parties would be needed before the treaty could enter into force. Primarily Budapest Convention member countries requested a higher number of signatories (70) before 'entry into force' of the treaty than Russia, China, Pakistan, Iran, India, Tanzania, Chad and Peru, who all proposed 30 signatories. While some states noted that past conventions such as the UNCAC went into force after 30 ratifications, the existing regional convention, the Budapest Convention, has 68 parties and 20 observer countries.[11] Singapore, which is neither a member nor observer to this convention, also agreed the UN convention should have higher ratification than Budapest, while some Budapest members and observers suggested a lower number, such as Japan and South Africa, so the differences were not a straight line. Some states attempted to find a middle ground. Thailand, for example, voiced support for 40 to 50 states, emphasizing the importance of rapid application, as Thailand is not party to any existing agreement. Mexico suggested it should be adopted with two-thirds majority, which aligns with the rules of the AHC process.



THE JANUARY MEETING

In January 2023, states convened to discuss chapters on criminalization, general provisions, and procedural measures and law enforcement cooperation. The meeting was similarly characterized by the two poles: those seeking wide state powers and few safeguards, and those seeking to limit the types of criminal activities covered in the treaty and binding them by safeguards. The polarity was evident in discussions on the breadth of crimes to include in the treaty, scope for cooperation on electronic evidence, the range and scope of procedural measures, and efforts to both slim down and remove language on safeguards and human rights, and, conversely, efforts to strengthen them.

On criminalization, there was a general agreement on the inclusion of cyber-dependent crimes, but different perspectives on the inclusion of other types of crimes. Certain sections in the negotiating draft had no basis for consensus and were moved into government informal meetings, where they are discussed behind closed doors.

This included the entire section on crimes such as incitement, extremism-related offences, terrorism-related offences and cyber-enabled crimes, which are found in other treaties, such as arms or drugs trafficking. There was vigorous opposition to including most of these sorts of crimes in the treaty (primarily brought by the WEOG states), while there was strong support for them from others, such as Russia and China. The current public working draft[12] has only added to the text, with other crimes such as prohibition to incitement to violence, fake news and trafficking in persons. There is no indication in the text of deletion requests, yet given the positions of governments, this will no doubt come up again. Mexico and South Africa have introduced paragraphs that recognize the need to address cyber-enabled crimes within the relevant existing instruments (outside this draft treaty), which appears to avoid duplication while still recognizing the relevance. This approach could avoid a list of duplicative crimes in this treaty and existing mechanisms.

Topics that moved to informals also included the thorny issue of terminology, such as defining computer data, which will eventually need to be decided upon and made consistent throughout the treaty. Several articles relating to online sexual exploitation, which broadened the topics, such as incitement to suicide, were also moved to private negotiations, as were articles on identity-related offences, violation of personal information and infringement of copyright.

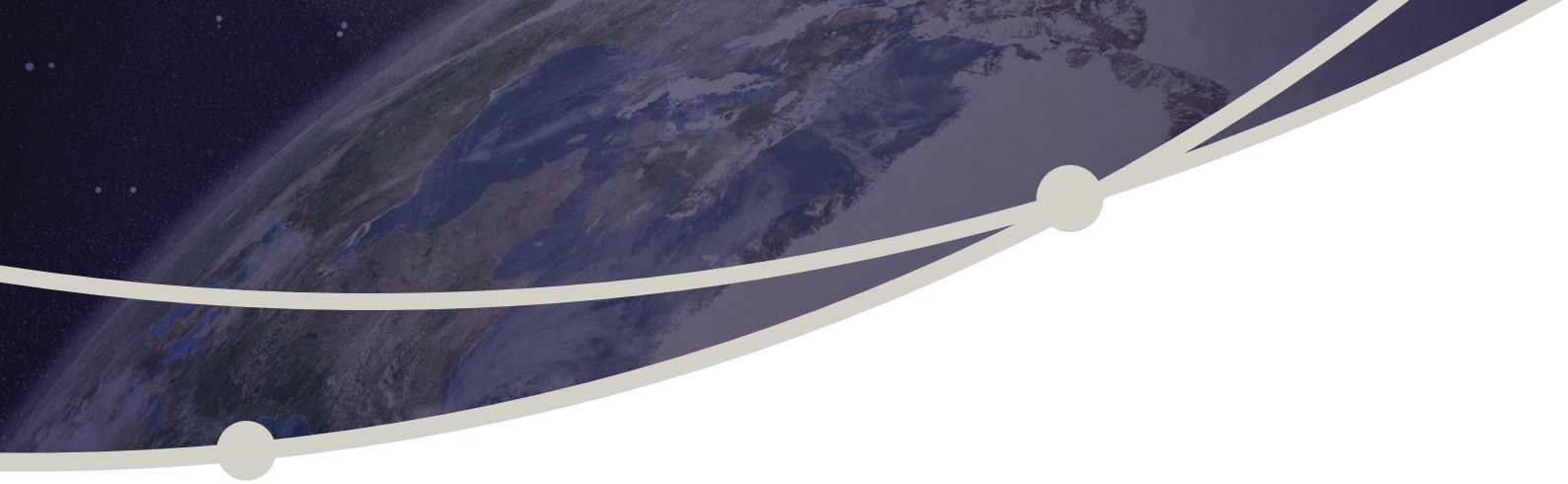
President Biden said that a Russian-based group was behind the ransomware attack that forced the shutdown of the largest oil pipeline in the eastern United States. *© Francois Picard/AFP via Getty Images*

Several issues under the chapter on procedural measures and law enforcement were also moved to informals, including jurisdiction, interception of content data, real-time collection of traffic data, and admission of electronic/digital evidence. In these it appears progress has been made on updating the language, but besides jurisdiction, there are still two sizeable lists calling for the full deletion or retention of the articles.[13]

CONCLUSION

The August 2023 meeting, intended to be the final in-person negotiation of the zero draft before a final draft treaty is adopted in early January 2024, will be a critical juncture in the development of this potential treaty. There are likely to be three main ways the negotiations might come together. One would be an attempt to usher states into one orbit or the other by offering incentives, such as in technical assistance. The second would entail efforts to bridge perspectives between the opposing poles by creating a treaty that it is believed can be both efficient and at the same time tempered by building in human rights safeguards. In the end, however, it is more likely that we will see a third scenario emerge: some key decisions will come down to a vote.

Alternatively, if none of these scenarios materialise, states might decide to kick the can down the road. Without movement on some of these issues, the AHC's current timeline, which requires adoption of a treaty in early 2024, will be in doubt and the AHC may have to make procedural decisions to mitigate that and extend the negotiations.



NOTES

1 In this brief, we use the term 'cybercrime' for the reason that it is a recognized phrase, is shorter and still captures the general framing of the treaty, even though precise terminology has not yet been settled.

2 Summer Walker and Ian Tennant, Wood for the trees, GI-TOC, 2 February 2023, https://globalinitiative.net/analysis/international-convention-ict-crime-ahc-un/.

3 The Budapest Convention on Cybercrime is a Council of Europe Convention with 68 parties and 20 observers or signatories.

4 UN General Assembly, Resolution adopted by the General Assembly on 26 May 2021, UN Doc. A/RES/75/282, 1 June 2021.

5 States within regional groups often take the floor with more specific and nuanced positions. Regional group inputs are where consensus is found among states in the group.

6 Being gay: Where it can lead to prison or even death, *Bangkok Post*, 29 November 2022, https://www.bangkokpost.com/life/social-and-lifestyle/2449144/being-gay-where-it-can-lead-to-prison-or-even-death.

7 Fifth session of the Ad Hoc Committee, 11–21 April 2023, Vienna.

8 Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, UN Doc. A/AC.291/19.

9 For an understanding of how capacity building could lead to misuse by states, see Cyber Policy Team, How can the cybercrime convention adopt a strategic approach to cybercrime capacity building and protect against potential harms and misuses? Chatham House, April 2023.

10 Fifth session of the Ad Hoc Committee, 11–21 April 2023, Vienna.

11 Council of Europe, Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY, https://www.coe.int/en/web/cybercrime/parties-observers.

12 Compilation document for Group B (status: 18 January 2023), working documents, fourth session of the Ad Hoc Committee, UNODC, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html.

13 Working document for Group D (status: 18 January 2023), working documents, fourth session of the Ad Hoc Committee, UNODC, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 600 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net