

POLICY BRIEF



**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

SPRING FORWARD

STATES TO REVIEW PART II OF
DRAFT CYBERCRIME TREATY

Summer Walker | Ian Tennant

APRIL 2023

ABOUT THE AUTHORS

Summer Walker is the Global Initiative Against Transnational Organized Crime (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 at the UN and with international NGOs, development agencies and research institutes.

Ian Tennant is based in Vienna, where he leads the GI-TOC's engagement with the UN Office on Drugs and Crime, and the wider diplomatic and civil society community in Vienna. He manages the GI-TOC's Resilience Fund, a multi-donor initiative that supports civil society individuals and organizations working to counter the damaging effects of organized crime around the world.

© 2023 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global Initiative.

Please direct inquiries to:

The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva

www.globalinitiative.net

Contents

Acronyms and abbreviations	2
SUMMARY	3
PREAMBLE	4
INTERNATIONAL COOPERATION	6
The consolidated negotiating draft.....	6
Procedural additions require a second look	7
TECHNICAL ASSISTANCE, INCLUDING INFORMATION EXCHANGE	10
Link between technical assistance and the implementation mechanism.....	11
MECHANISM OF IMPLEMENTATION	12
CONCLUSION.....	17
Notes	18



Acronyms and abbreviations

AHC	Ad hoc committee
CCPCJ	UN Commission on Crime Prevention and Criminal Justice
COSP	Conference of states parties
ECOSOC	UN Economic and Social Council
ICT	Information and communications technology
ITC	International technical commission
ITU	International Telecommunications Union
MLAT	Mutual legal assistance treaty
UNCAC	UN Convention Against Corruption
UNODC	UN Office on Drugs and Crime
UNTOC	UN Convention against Transnational Organized Crime



SUMMARY

In April 2023, the UN ad hoc committee to elaborate a convention on the ‘criminal misuse of information and communications technology’ will meet for its fifth session to discuss the second half of its consolidated negotiation draft. This will result in a zero draft convention, to be presented to states and stakeholders in August 2023 as the march towards a new convention continues. In January, the ad hoc committee (AHC) concluded its review of the first half of the consolidated negotiation draft, which was produced by the AHC Chair. The draft was considered and red-lined in detail throughout the session, a typical process for governments to modify resolutions and draft treaties. However, as governments hammered out details line by line, the review process revealed a continued lack of understanding around some of the basics of the treaty.

The GI-TOC was left with a sense of concern over how wide the potential scope of the treaty was becoming, which means it could be used as a tool for repression as much as a tool for combatting cybercrime in the future.¹ A related concern was the pushback against the inclusion of legal safeguards, not just from the usual cast of governments, but also from crucial blocks such as the Caribbean Community. We feel it is too early in the negotiating process to lose ground on legal safeguards, especially as there seem to be no limits to the scope of cooperation, at least at this stage. As we have noted in the past, an international criminal justice instrument requires legal safeguards, and it is of heightened importance given this is the first global cyber-focused treaty.²

In this brief we analyze the second half of the negotiating draft, focusing on the four chapters that will be considered at the fifth session in April: the preamble, international cooperation, technical assistance and implementation mechanisms. The draft also includes chapters on prevention and final provisions, which we do not explore in this brief.

Overall, we find that:

- These chapters are bound much more clearly by the (still undefined) criminalization chapter, with language that establishes this. If these links stay in place, it will contribute to the agreement of a treaty with a limited scope, which would be established in the criminalization chapter.
- Unlike the chapter on law enforcement and procedural measures, there is more consistent inclusion of particular legal safeguards attached to relevant articles. Some of this is taken directly from agreed upon UN language, such as the UN Convention against Transnational Organized Crime (UNTOC), and some of it is brought in from government submissions. More can be done to strengthen language and references for these safeguards, but the inclusion throughout is welcome.
- There are some hot-button issues, such as the introduction of new procedural measures that are unrelated to cybercrime specifically, as well as long-standing issues such as cross-border access to data, which are likely to raise debate in the plenary.
- Technical assistance will be a welcome chapter, but likely to be viewed as too prescriptive and detailed for some governments. Thus, suggestions to pare it down during negotiations are likely.



PREAMBLE

The preamble is currently a combination of language taken from government submissions, so there is some redundancy and conflation of issues. In April, one of the objectives of delegates will be to streamline this language during government negotiations.

Paragraph 2 provides an overall framing on why the treaty is important in service of other societal goals, including the three pillars of the UN. There are an additional two paragraphs referencing the well-being and protection of society. This type of framing is supportive of a greater good, yet one reference would be sufficient. There are paragraphs that recognize the imperative of this treaty to promote an open and secure cyberspace, as well as to protect personal data, which again help situate this document in a larger context of digital responsibilities. We welcome the language upfront in the preamble recognizing a role for the private sector, academia and civil society in working towards the treaty's goals.

There is some redundancy in the discussion of transnational organized crime. One paragraph notes concern about the links between cybercrime/criminal misuse of information and communications technology (ICT) and transnational organized crime, while another states that cybercrime/criminal misuse of ICT 'constitutes transnational crime'. Between these two options, it makes most sense for the convention to retain the first paragraph expressing concern over links with transnational organized crime, rather than the second. The second makes an assumption that is not helpful for policy responses. If the convention retains the terminology 'the use of information and communications technologies for criminal purposes', all things falling under this category would constitute transnational organized crime, a claim that is far too broad. Similarly, if cybercrime is used, option two again would claim all instances would constitute transnational organized crime, which would capture that domestic acts, small-scale cybercrime and non-organized individual act all as transnational organized crime – which is unhelpful for analysis and for policy.

There will also be negotiations on technical language that may be seen as too weak or too strong in some cases. For example, in the first paragraph, the AHC has chosen the phrase 'bearing in mind' when connecting this treaty to the UN Charter, whereas treaties under the UN should have a more direct link to the charter, given its primary status within the UN. The language in the sovereignty paragraph is weaker than the agreed upon UN language used in previous treaties and is likely to be raised in the plenary by China and others, who will want to see it strengthened.

There is also language that has been viewed as problematic in other UN crime-related fora, which have called for a balancing between the interests of law enforcement and human rights. Law enforcement is a sector of government that enforces laws and public safety, whereas human rights are an overarching framework of concepts and laws, including those enshrined in the UN Declaration on Human Rights, that endow 'rights inherent to all human beings'.³ To balance them would be an unfair comparison. Rather, law enforcement – and all other sectors – should operate within a human rights framework.



GI-TOC RECOMMENDATIONS: PREAMBLE

UN Charter

'Bearing in mind' should be replaced with 'Guided by' (such as in the Arms Trade Treaty) in paragraph 1.

Transnational organized crime

Recommend retaining paragraph 4 on links and deleting paragraph 7 claiming '[cybercrime] [the use of information and communications technologies for criminal purposes] constitutes transnational crime'.

Society

Recommend retaining paragraph 3 and deleting paragraph 6.

Sovereignty

Revert to agreed upon UN language on sovereignty in paragraph 12.

Human rights

In paragraph 15, remove introductory language 'Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for human rights'. Retain the remaining paragraph.



INTERNATIONAL COOPERATION

Research has found that international cooperation on criminal justice matters is disjointed and reactive, particularly in the face of diminishing support for multilateralism.⁴ For instance, despite near universal adherence to the UNTOC, evidence that it has enhanced international cooperation is hard to find.⁵ One study found that, overall, ‘international treaties have mostly failed to produce their intended effects’, with the exception of trade and finance treaties.⁶ The challenge is that, in reality, the treaty text may not enhance international cooperation.

Regional treaties, such as the Council of Europe’s Budapest Convention on Cybercrime, appear to have stronger cooperation between largely like-minded groups of countries. One key lesson from the UNTOC is that there is little evidence of enhanced cooperation between countries who had not already built up their own relationships and cooperation mechanisms independently – whether through historic ties, cultural or political affiliation, or existing law enforcement relationships.⁷

International cooperation in criminal matters faces serious issues when it comes to human rights safeguards, another reason why cooperation between diverse countries has not flourished. For this reason, safeguards articles are needed throughout the treaty, as various multistakeholders have called for in their submissions.⁸

Successful cooperation requires improved transparency, accountability and oversight, which could be enhanced through the reporting process on these provisions. This is a point at which the open and inclusive civil society engagement modalities could be employed by the convention following its adoption.

The consolidated negotiating draft

Many anticipated aspects of cooperation, such as extradition and mutual legal assistance, are included in this chapter. The general principles of international cooperation state that the goal of cooperation is two-fold: to disrupt the crimes listed under the future convention and to collect electronic evidence. The option posed to states is whether collection of evidence should be for offenses within the convention or a wider set, such as serious crimes. We recommend limiting cooperation to crimes covered by the treaty. The general principles also include a clause allowing states to collaborate on civil and administrative matters, which derives from the UN Convention Against Corruption (UNCAC), and its role in this treaty is not obvious. Article 56.4 makes the chapter subject to the safeguards in article 42, creating linkages across the treaty.

Article 57 on protection of personal data will cause debate as regional perspectives differ on the content of these protections. There will be questions around how prescriptive these articles should be, versus how much decision power should be in the hands of state requesting and granting authorities. There is a question as to how detailed this section should be based on: (1) the ability of states to select the most advantageous elements of existing data protection law while leaving out key protection provisions, and (2) the ability of states to interpret the future clauses in a way that fits their political objectives beyond the convention.⁹ Therefore, some multistakeholders and others may recommend a limited section based on key principles.

The basis for extradition and mutual legal assistance in this draft were taken from the UNTOC, with additions based on government submissions to the process. Most of the clauses on extradition are unlikely to raise eyebrows. The extradition section begins by stating that extradition is possible for the criminal offenses outlined in the treaty (which are still being negotiated). This would create a narrow framing for extradition, depending on the final criminalization chapter. It sets a limit of one year (minimum) deprivation of liberty for extradition, which is a low

threshold. Paragraph 1 of article 58 requires dual criminality, but paragraph 2 creates an exemption for states if they chose to – this contradiction should be remedied and dual criminality should be a requirement.

The section includes a clause on grounds for refusal taken from the UNTOC (article 58.15), and adds rejection based on the risk of torture. While this includes ‘political opinions’ as one reason to reject extradition, paragraph 4 has text taken from the Russian draft submission saying that states using this treaty for the basis of extradition shall not consider the offenses in this treaty as political offenses, seemingly closing off the option of refusal based on political grounds. These contradictions will need to be resolved in negotiations. Model treaty text from the UN Office on Drugs and Crime (UNODC) on extradition offers language that refusal can result ‘if request is regarded by the requested State as an offence of a political nature’,¹⁰ which could be used in this context.

On mutual legal assistance, again the basis is the UNTOC, but it includes additions based on the cyber focus of the treaty. When listing the purposes for requesting a mutual legal assistance treaty (MLAT), it expands upon the UNTOC’s established list with items such as searching and seizing computer data, collecting real-time traffic and collecting or recording content. The parameters for these tasks will be defined in the earlier chapter ‘Procedural Measures and Law Enforcement’, which was first discussed in January.

States will largely support the 24/7 network proposed (a mechanism to provide immediate assistance). Many have voiced support for this type of initiative during previous negotiations. INTERPOL has also raised its existing 24/7 network as a place that can house such a network for this convention. Given that such a network would be established under the auspices of the UN, it will be paramount that this treaty does not allow for it to be weaponized as a tool of transnational repression against activists, journalists and political opponents by limiting the crimes for which it is able to operate.

Article 72 on cross-border access to data will be a contested article, in particular clause (b), which allows governments to obtain data directly from individuals (private companies) in another state’s territory without government consent. The inclusion of this item in the Budapest Convention was Russia’s main reason for not acceding to the convention. China is strictly against such an option in a treaty and has clearly stated that in negotiations. These states do not want governments to obtain data stored in their territories from service providers without government consent.

Article 76 on public–private partnerships to enhance investigations is likely to draw concern from the private sector. The current wording is very state-centric and could possibly be interpreted as having the power to compel private sector companies to cooperate in cross-border investigations. The Electronic Frontier Foundation and Privacy International, for instance, have recommended that this article include protections via Article 42 on safeguards.¹¹

Procedural additions require a second look

There are several procedural articles in this section that raise some concerns within a cyber treaty. These include

- Article 62. Conducting interrogations and other procedural actions using video or telephone conferencing systems;
- Article 65. Powers of diplomatic missions and consular offices; and
- Article 66. Emergency mutual legal assistance.

Some of these are aimed at changing how international diplomacy is done. Interjecting changes in how diplomatic missions operate globally would be outside the scope of this treaty and would undermine the role of diplomatic missions, while fuelling the opportunity for transnational repression.

An article on special investigative techniques (article 78) is largely based on article 20 of the UNTOC and calls for



creating bilateral or multilateral agreements under the future convention to cooperate in online surveillance and undercover operations. It includes a reference to carrying out such efforts in line with evidence being admissible in court, however, there are still red flags over its role in this cyber treaty. Although this article exists in a non-cyber treaty, its inclusion here could normalize government surveillance as a matter of cybercrime policy.

An article on 'spontaneous information' (article 64) also appears superfluous as the MLAT process is the basis for cooperation and there is an additional article on emergency MLATs. The articles are intended to improve speed of cooperation but open the door to rapid sharing of computer data without safeguards and with loopholes for due process violations. Across the section on MLAT, judicial oversight should be a key component of international cooperation.

GI-TOC RECOMMENDATIONS: INTERNATIONAL COOPERATION

General principles

Article 56. General principles of international cooperation

Paragraph 1: Recommend limiting collection of e-evidence to 'offenses set forth in this Convention'.

Extradition

Article 58.4 contradicts language in Article 58.15. Recommend deleting the last sentence of Article 58.4.

Recommend the inclusion of a concrete paragraph on mandatory grounds for refusal if 'request is regarded by the requested State as an offence of a political nature'.¹²

Mutual legal assistance

Article 61. General principles and procedures relating to mutual legal assistance

Paragraph 1: Recommend limiting collection of e-evidence to 'offenses set forth in this Convention'.

Paragraph 19: Recommend this section include the clause from extradition based on non-discrimination.

Article 64. Spontaneous information

Recommend that article should be deleted.

Article 65. Powers of diplomatic missions and consular offices

Recommend that article should be deleted.

Article 78. Special investigative techniques

Recommend that article should be deleted.



THE RISK THIS TREATY COULD SUPPORT TRANSNATIONAL REPRESSION

As negotiations proceed, the GI-TOC has identified one clause as posing the greatest risk to advancing a treaty that could be instrumentalized to support transnational repression. Transnational repression is defined by NGO Freedom House as a process ‘in which governments reach across national borders to silence dissent among their diaspora and exile communities’.¹³ Advancements in technology have brought great benefits to our society, but in its global connectivity, technology has also increased the ability of states and groups of states to surveil and target people outside their borders.

The main risk in current negotiations is the potentially wide scope for cooperation among governments, facilitated by international agencies and bodies. Some of this risk lies in how broad the forthcoming criminalization chapter could be in setting out a list of core crimes addressed by the treaty. But the major red flag is text allowing governments to use the treaty to collect electronic evidence for any crime or serious crime, rather than a delimited list of crimes defined within the treaty. The language granting governments the potential to cooperate on a limitless range of crimes currently is in article 41, on scope of procedural measures, and article 56, on general principles of international cooperation.

Depending on the scope of cooperation, two willing governments (or a group of countries), could use an international criminal justice treaty in the following ways:

- They could compel companies to collect and hand over data on political dissidents, journalists or other persons of interest to governments. These could be citizens or foreign nationals.
- They could utilize infrastructure created by this treaty, such as a 24/7 network, to request data for rights-violating agendas, such as anti-LGBTQI agendas.
- They could encourage – or even compel – international agencies to cooperate in these efforts.
- They could base extradition requests of political dissidents on domestic cyber laws, such as disturbing public order or defaming a political figure online, using dual criminality as the justification (potentially dependent on the final criminalization chapter).

There remain additional articles of concern, such as ‘Special investigative techniques’, but the crux of the issue will remain even with the removal of these types of articles. If cooperation remains wide open on all crimes for technical matters, the treaty may not have the mechanisms needed to prevent the threat to human rights and freedom of expression.



TECHNICAL ASSISTANCE, INCLUDING INFORMATION EXCHANGE

Chapter V is of key importance to many Latin American and African states, who have voiced throughout negotiations the need to improve their domestic ability to combat both cybercrimes and cyber attacks in order to cooperate internationally. The general principles of the technical assistance chapter are aimed at the needs of the Global South and include a clause on a holistic approach to capacity building that includes ‘sustainability, transparency and accountability’.

In the general principles (article 86), paragraph (b) is likely to undergo some debate: ‘Each beneficiary shall determine its own priorities, based on country-specific situations and requirements’. It is a welcome addition in that it promotes national ownership of capacity building, but it could also be interpreted as saying that technical assistance is a bilateral effort between UN agencies and requesting states. This may be viewed as going around the typical process, which is driven by resolutions and priorities determined by, for example, a future conference of parties. In addition, available funding is always key to the provision of technical assistance through the UN. Relatedly, Global North countries will probably view the inclusion of ‘economic development’ in the title of article 89 as outside the scope of this convention.

The chapter includes a list of activities for potential training programmes needed to improve efforts to combat cybercrime, with a focus on law enforcement training. This should be complemented with clauses for judicial training, which is already included in terms of witness protection, for instance, but should play a larger role throughout the section. The inclusion of training on data protection and privacy protection will be critical if a future convention is going to be implemented in line with citizen security and human rights. Training to mainstream a gender perspective in policymaking, legislation and programming is welcome as an early mandate for technical assistance in this area.

Several countries have followed Brazil’s suggestion to submit their capacity-building needs to inform the development of this chapter. The Czech Republic has submitted a document offering support; Colombia has listed what it can offer and some of its needs; and Ecuador, Kyrgyzstan and Mauritius have submitted their specific needs.¹⁴ The offers include law enforcement training such as investigative techniques, as well as knowledge sharing such as sharing best practices.

The requests for training and support may begin to exceed what governments are willing to cooperate on – and fund. Some of the more typical assistance provided by agencies like the UNODC, such as developing legislative frameworks and law enforcement training like digital forensics, are included. The submissions also contained more unique needs, such as for specialized equipment, facilitating memorandums of understanding with social media companies, decryption of messaging apps or cryptomining. Although there is no harm in sharing these needs as part of the exercise, many are likely to end up outside the scope of a treaty, depending on the final parameters. This exercise does, however, show that the aspirations for the technical assistance provided by this treaty are unlikely to match up against the realities of funding, implementing partner expertise and general bandwidth in the UN system.



Given the wide range of potential capacity-building measures, article 89.10, which calls for transparent monitoring and evaluation of all assistance activity, is a welcome inclusion for two reasons. First, it is important to determine which training initiatives are effective. Second, given the sensitivities of cyber/tech capacity-building – and the possible inclusion of technology transfers through the UN – it is critical to create a transparent environment for stakeholders across sectors to understand the UN’s role in this.

Link between technical assistance and the implementation mechanism

The implementation mechanism is an important factor for future technical assistance. If the AHC adopts a mechanism modelled solely on the UNTOC or UNCAC, there is a risk that the processes will focus exclusively on developing countries as the beneficiaries of the ‘technical assistance’ afforded by the secretariat (the UNODC for UNTOC and UNCAC), which is dependent on funding from donor countries. Although this action would respond to the clear needs and requests for enhanced capacity-building from some countries, one unintended consequence could be an incorrect perception that the crimes under the convention are a problem of the Global South, to be fixed by financial support from the Global North.



MECHANISM OF IMPLEMENTATION

Implementation mechanisms ensure that treaties are actually put to use. They are how governments convene to discuss implementation and update treaties through the process of adopting new resolutions. This is where governments direct technical assistance, address new threats, update procedures and policies, and assess whether the treaty is still responding to real-world conditions. Most recent treaties also include a review mechanism that asks governments to report on their progress in treaty implementation. In one study from 2022, implementation mechanisms were assessed as the only modifiable treaty design choice with the potential to improve the effectiveness of treaties.¹⁵ This is therefore an important chapter to get right. The draft contains three options for implementation and does not set out options for a review mechanism, but rather notes a review mechanism should be determined after ratification by the body established as the implementation mechanism.

The draft proposes three options for a mechanism of implementation:

- **Option 1** proposes a similar mechanism to the UNTOC and UNCAC, with a conference of parties.
- **Option 2** has the same basic proposal, but with an added ‘International Technical Commission’, which would comprise a smaller group of members and would link the conference of parties to the International Telecommunications Union (ITU).
- **Option 3** proposes absorbing the conference under the purview of the UN Commission on Crime Prevention and Criminal Justice (CCPCJ).

None of the options references human rights, or includes references to human rights monitoring mechanisms or processes. Given the particular risks involved in cybercrime legislation and human rights, this is particularly troubling and should be resolved as negotiations progress. Below we assess each option and provide our recommendations, including recommended language, for an implementation mechanism:

Option 1 offers the same formula as the UNTOC and UNCAC with the primary purpose of improving capacity and cooperation between states parties. This is important but does not include the additional purpose of generating evidence and analysis, and fostering multistakeholder engagement on that evidence. Given the fast-moving nature of the crimes to be included under the treaty, data analysis should be emphasized and included as a driving purpose, rather than just an activity, as currently drafted. The section has references to NGOs, but no clear modalities for their inclusion. This could easily limit the range of expertise involved, since the UNTOC and UNCAC model automatically allows UN Economic and Social Council (ECOSOC)-accredited NGOs¹⁶ and invites others to be included, although their invitations can be objected by states. This would contrast with the wide range of expertise afforded by the open and inclusive methods of the AHC.

Option 2 offers the same conference of states parties (COSP), but with an international technical commission (ITC). As it is currently drafted, the ITC would be a permanent body of experts with two-thirds of members representing the COSP, and one-third representing members of the ITU, the UN’s specialized agency for information and communication technologies. The ITU is a technical body and linking it so closely to a criminal justice treaty could lead to the politicization of its work. In the past, states have used the ITU to try to advance encryption-breaking and other politically motivated tech goals.¹⁷ Given the wide range of relevant actors within the UN system, this option would require a broader group of UN agencies to be included. For instance, the UNTOC COSP and the UN Office for the High Commissioner on Human Rights, which contains several special rapporteurs on technology issues, would be relevant bodies. An ITC should also include space for inputs from regional bodies with relevant conventions or processes, such as INTERPOL, the Council of Europe and its Cybercrime Convention Committee.

Presumably, the ITC's experts would be comprised of multistakeholders, as it states: 'The members of the Commission [ITC] shall be experts with significant direct experience in international relations, international and criminal law, communications technologies or relevant related research.'¹⁸ A similar model is the UN's International Narcotics Control Board, where 10 of its members are nominated by their governments and three by the World Health Organization, and, once elected, they serve in their individual capacity (though there can be lingering concern of government influence).¹⁹

The text could clarify that the ITC experts are non-governmental experts coming from the multistakeholder community, offering an innovative and inclusive format for long-term and technical engagement.

Option 3 proposes housing the implementation mechanism under the CCPCJ, which is a functional commission of ECOSOC. The approach offers a relatively flexible way of implementing a COSP and a review mechanism with realistic reporting goals (states report every five years). It builds on the experience of the previous intergovernmental expert group on cybercrime, which has been housed under the CCPCJ since its creation by the UN Crime Congress in 2010. This formula prioritizes the exchange of information among the convention parties and includes a reference to coordination with other multilateral and regional bodies.

The major risk of this option is inclusion, and it would need to be bolstered by clear modalities to ensure inclusivity. Many member states are not present or active in Vienna, where the CCPCJ is hosted. This has been a running issue since the inception of the AHC, which led to AHC meetings in both Vienna and New York for inclusion. While it could be beneficial to host the discussions in Vienna in terms of substantive expertise, some countries would be excluded. The limited membership of the CCPCJ²⁰ and ECOSOC²¹ means voting power would only rest with a handful of countries. The other main issue with regards to inclusion is multistakeholders. The CCPCJ is only open to ECOSOC-accredited NGOs and many AHC stakeholders are not accredited to ECOSOC. This option should be updated to ensure inclusive modalities, stronger language on meaningful engagement with other UN bodies and modified language on multistakeholders to avoid following the CCPCJ's path of ECOSOC-only NGOs.

GI-TOC RECOMMENDATIONS: IMPLEMENTATION MECHANISM

Whichever option is selected, our recommendation is to create rules that ensure wide participation of interested stakeholders. Existing modalities for multistakeholder engagement within the AHC could apply to the mechanism of implementation, with regular calls for new multistakeholders to attend meetings of the mechanism.

There is also a very important safeguard built into the AHC process, which is a two-thirds voting majority when consensus cannot be reached. Implementation will have resolutions that update the principles and priorities of the treaty, and it is recommended that the two-thirds voting mechanism is carried over.

Below is the GI-TOC's proposed language for an implementation mechanism, which would need to be adapted depending on the physical location and links with other UN mandates.

1. *The states parties of the convention shall create a mechanism of implementation to be created with the purposes of:*

a. *Analyzing, in a consultative process including states parties, relevant UN agencies and multi-stakeholders, trends in cybercrime/crimes included in this treaty, the circumstances in which they take place, and the actors and technologies involved in committing such crimes.*

b. *Building trust and fostering engagement between states parties, and between states parties and multistakeholders as part of efforts to implement the international cooperation provisions of the treaty.*

2. *The mechanism shall facilitate the development and sharing of analytical expertise concerning cybercrime/crimes included in this treaty amongst states parties and multi-stakeholders.*

3. *As part of the mechanism, states parties and multi-stakeholders shall monitor the policies and measures put in place by states parties to implement the treaty and make assessments of their effectiveness and efficiency.*

4. Policy guidance, capacity building and technical assistance delivered to implement the treaty shall be informed by the data and evidence shared under the auspices of the mechanism, and shall be designed for use on varied contexts, in both Global North and Global South countries.

5. The mechanism shall be open to all Parties and Multistakeholders, and constitute the following agenda items in its meetings:

- i. **Effectiveness and Efficiency.** To consider the efficiency and effectiveness of the work of the Convention, through states reporting on their own implementation and multistakeholder perspectives on implementation. To make recommendations on future modifications to the Convention and its implementation mechanism.
- ii. **Strategic Coordination.** To ensure that the implementation mechanism is making maximum use of coordination opportunities with other multilateral partners. Inclusion of representation and engagement with UN Commission on Crime Prevention and Criminal Justice (CCPCJ) and the UN Human Rights Council, International Telecommunications Union (ITU), Interpol, Council of Europe [and others] on progress, and to make recommendations on improvements.
- iii. **Trends and Analysis.** [inspired by per Article 28 of UNTOC and Article 61 of UNCAC]. To allow for presentation and discussion of the latest trends and evidence in the dynamics of crimes under the convention, and state and multistakeholders would make presentations on the latest findings and their implications for the implementation of the Convention.
- iv. **International cooperation:** Sharing of evidence and best practice on concrete cases of international cooperation that have taken place due to the convention, to include analysis of the extent to which the Convention is facilitating cooperation, and make recommendations based on those findings.
- v. **Policy guidance and technical assistance:** To give all states access to information and resources needed to better implement the Convention, whether they are from the Global North or Global South.
- vi. **Human rights, data protection and effectiveness of safeguards.** To ensure that the convention's implementation does not compromise human rights, data protection and other safeguards. Breaches of safeguards and human rights organizations would be reported and debated under this item.

9. The modalities for multi-stakeholder engagement in place for the AHC shall form the basis for the multistakeholder participation modalities of the mechanism of implementation, with regular calls for new multi-stakeholders to apply to attend meetings of the mechanism. Therefore:

- i. Representatives of relevant global and regional intergovernmental organizations, including representatives of United Nations bodies, specialized agencies and funds, as well as representatives of functional commissions of the Economic and Social Council, shall attend the meetings;
- ii. Representatives of non-governmental organizations that are in consultative status with the Economic and Social Council, in accordance with Council resolution 1996/31 of 25 July 1996, may register with the secretariat in order to participate in the sessions of the implementation mechanism;
- iii. Other relevant non-governmental organizations, civil society organizations, academic institutions and the private sector, including those with expertise in the field of crimes under the convention, may participate in the mechanism, taking into account the principles of transparency and equitable geographical representation, with due regard for gender parity, shall register to attend, on a non-objection basis.
- iv. With regards to participation, all decisions by States Parties concerning the Mechanism, without approval by consensus shall be taken by a two-thirds majority.



UNTOC AND UNCAC CONFERENCES AND REVIEW MECHANISMS: MULTISTAKEHOLDER PARTICIPATION

This treaty text (and the secretariat's review of existing mechanisms²²) takes inspiration from the UNTOC and UNCAC conferences, which have very similar conferences of parties and review mechanisms, but operate completely separately. Given the GI-TOC's experience with those review mechanisms, we would suggest that this negotiation offers an opportunity to think differently and take a new approach.

The UNTOC and UNCAC essentially lead separate lives, operating under separate conference bodies, maintaining different secretariats and having distinct review mechanisms that are not coordinated. The absence of coordination and exchange is exacerbated by the lack of formal roles for civil society within the review mechanisms. A further issue is that civil society is not included in the subsidiary bodies of both conferences.

We have identified three structural problems in the design of these mechanisms:

Due to the separate implementing regimes, the international community is unable to understand the overarching dynamics, inter-relationship and impact of organized crime and corruption, especially as expert voices are restricted.

States become overwhelmed with the bureaucratic processes that govern the conventions, including the review mechanisms. States are in the midst of a long-term review process with an unknown length of time left, and have already spent 13 years working on the UNCAC's review mechanism. At the same time, they have recently embarked on another colossal UNTOC review mechanism that is a minimum 10-year process, with unknown time and resource implications.

The work that is undertaken lacks transparency and accountability, as the country reviews under each review mechanism can be edited by the party under review and elements of information can be kept hidden from public view.

Regarding civil society participation, the GI-TOC analyzed the two conventions of UNCAC and UNTOC and made the following observations in a recent policy brief:²³

UNCAC COSP

- NGOs with ECOSOC status are invited to attend the UNCAC COSP, and other relevant NGOs may apply to attend the regular meetings. However, since the adoption of the UNCAC in 2003 and its implementation review mechanism in 2009, civil society has faced a consistent and growing set of obstacles.
- The 'Marrakesh compromise', struck at the 2011 COSP in Morocco, sets the rules for NGO engagement.²⁴ Under the compromise, NGOs can attend the main sessions of the UNCAC COSP but cannot attend the COSP's subsidiary bodies, including the working group that meets to monitor the implementation of the convention.
- An 'NGO briefing' has been instituted, where civil society and states can meet on the margins of the Implementation Review Group. However, NGOs that attend may not mention 'country situations', i.e. what is happening with corruption or UNCAC implementation in any specific country.
- The main UNCAC conference has also suffered from a growing trend of states parties objecting to the attendance of specific non-ECOSOC NGOs.

UNTOC COSP

- The implementation of the UNTOC at the multilateral level is overseen by its own COSP, which counts almost all countries as members, at 190. Like the other policymaking bodies under the auspices of the UNODC, it operates under the Vienna spirit of decision-making, effectively handing states a veto if they wish to wield it. This helped ensure that the conference did not adopt a review mechanism until 2018, a full 15 years after the treaty entered into effect.
- The issue of civil society participation, along with the mechanism's financing, was a major sticking point for delegates who could not agree on an appropriate review mechanism to measure and improve implementation of the convention. The compromise that was finally reached in 2018 was modelled on the UNCAC review mechanism, which included the 2011 Marrakesh compromise. It had a clearly defined role for civil society, although with high levels of restrictions and low levels of transparency.
- The Marrakesh compromise also inspired the UNTOC's 'Constructive Dialogues' that allow for generic engagement between states and non-governmental actors in the margins of the UNTOC conference. The review mechanism followed the practice of denying NGOs access to subsidiary bodies, which in this case includes the conference's working groups on trafficking in persons, smuggling of migrants, trafficking in firearms, and international cooperation and technical assistance.
- NGOs that do attend the Constructive Dialogues are subject to strict requirements as to what they can and cannot say (again, specific country situations cannot be mentioned).
- The GI-TOC policy brief analyzes the role of ECOSOC status in restricting civil society access to ECOSOC subsidiary bodies – including the UN Commission on Narcotic Drugs and the CCPCJ.²⁵

CONCLUSION

Following the meeting in April, both sections of the draft will have been reviewed by the AHC. The zero draft will then be presented to states and stakeholders in August 2023. The drafters will face three main challenges: winnowing down a very long text while keeping the essence of what states agree upon; choosing winners and losers by keeping or deleting sections on issues that are contentious between states; and making decisions on topics that had been moved to informal discussions because there was no foundational agreement between states on proposed text or concepts. August will be the moment when we find out, for instance, if the treaty becomes a ‘cybercrime’ treaty or a treaty on the ‘criminal misuse of information and communications technology’. In August, with a full draft, observers will also be able to determine the likelihood that governments are prepared to come together around the conceptual framework of the treaty, namely the crimes covered in the treaty and the scope of cooperation. This includes a careful consideration of possible unintended consequences and the norm-setting potential of the treaty as it relates to either cybercrime or crimes committed using information and communications technology.



Notes

¹ Summer Walker and Ian Tennant, Wood for the trees, GI-TOC, 2 February 2023, <https://globalinitiative.net/analysis/international-convention-ict-crime-ahc-un/>.

² Ibid.

³ See United Nations, Human Rights, <https://www.un.org/en/global-issues/human-rights>.

⁴ Yvon Dandurand and Jessica Jahn, The future of international cooperation against transnational organized crime: The undoing of UNTOC?, GI-TOC, October 2021, <https://globalinitiative.net/wp-content/uploads/2021/10/GITOC-The-future-of-international-cooperation-against-transnational-organized-crime.pdf>.

⁵ Ian Tennant, The promise of Palermo: A political history of the UN Convention against Transnational Organized Crime, GI-TOC, December 2020, <https://globalinitiative.net/analysis/the-promise-of-palermo-untoc/>; See also a review of the UNTOC's impact in Africa, a forthcoming GI-TOC report.

⁶ Steven J. Hoffman et al, International treaties have mostly failed to produce their intended effects, *Proceedings of the National Academy of Sciences*, 119, 32, <https://www.pnas.org/doi/10.1073/pnas.2122854119>.

⁷ Ian Tennant, UNCivil society: Addressing the diminishing space for civil society in UN policymaking bodies on transnational crime, Global Initiative Against Transnational Crime, October 2022, <https://globalinitiative.net/wp-content/uploads/2022/10/GITOC-UN-Civil-Society-11-UNTOC-COP-2022.pdf>.

⁸ UNODC, Various multistakeholder submissions, Fifth session of the Ad Hoc Committee, 2023, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main.

⁹ Findings from an expert round table held by the GI-TOC, 30 March 2023.

¹⁰ UNODC, Revised manuals on the model treaty on extradition and on the model treaty on mutual assistance in criminal matters, 2002, p 13, https://www.unodc.org/pdf/model_treaty_extradition_revised_manual.pdf.

¹¹ Electronic Frontier Foundation and Privacy International, Comments on the consolidated negotiating document of the UN cybercrime treaty: Chapters on international cooperation, technical assistance, and proactive measures, March 2023, p 12, <https://privacyinternational.org/sites/default/files/2023-03/PI%20and%20EFF%20submission%20UN%20CybercrimeTreaty-International-Cooperation.pdf>.

¹² UNODC, Revised manuals on the model treaty on extradition and on the model treaty on mutual assistance in criminal matters, 2002, p 13, https://www.unodc.org/pdf/model_treaty_extradition_revised_manual.pdf.

¹³ 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.

¹⁴ At the time of writing. More submissions may have been submitted since.

¹⁵ Steven J. Hoffman et al, International treaties have mostly failed to produce their intended effects, *Proceedings of the National Academy of Sciences*, 119, 32, <https://www.pnas.org/doi/10.1073/pnas.2122854119>.

¹⁶ See NGO Branch, UN Department of Economic and Social Affairs, Basic Facts about ECOSOC Status <https://csonet.org/index.php?menu=17>.

¹⁷ Findings from an expert round table held by the GI-TOC, 30 March 2023.

¹⁸ Article 94 bis, paragraph 3 of the consolidated negotiating document.

¹⁹ See International Narcotics Control Board, The International Narcotics Control Board, <https://www.incb.org/incb/en/about.html>.

²⁰ The CCPCJ has 40 members: Twelve from African states, nine from Asian states, four from Eastern European states, eight from Latin American and Caribbean states, and seven from Western European and other states.

²¹ ECOSOC membership is based on geographic representation: Fourteen seats are allocated to Africa, eleven to Asia, six to Eastern Europe, ten to Latin America and the Caribbean, and thirteen to Western Europe and other areas. Members are elected for three-year terms by the General Assembly.

²² UNODC, Mechanisms of implementation established under selected multilateral treaties - Note by the Secretariat, 10 March 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/2304514E.pdf.

²³ Ian Tennant, UNCivil society: Addressing the diminishing space for civil society in UN policymaking bodies on transnational crime, Global Initiative Against Transnational Crime, October 2022, <https://globalinitiative.net/wp-content/uploads/2022/10/GITOC-UN-Civil-Society-11-UNTOC-COP-2022.pdf>.

²⁴ UNCAC Coalition, Civil society locked out at UN anticorruption summit, calling effectiveness of global convention into question, 28 October 2011, <https://uncaccoalition.org/civil-society-locked-out-at-unanti-corruption-summit-calling-effectiveness-of-globalconvention-into-question/>.

²⁵ Ian Tennant, UNCivil society: Addressing the diminishing space for civil society in UN policymaking bodies on transnational crime, Global Initiative Against Transnational Crime, October 2022, <https://globalinitiative.net/wp-content/uploads/2022/10/GITOC-UN-Civil-Society-11-UNTOC-COP-2022.pdf>.