GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

HITTING PAUSE

THE UNFINISHED STORY OF THE UN CYBERCRIME NEGOTIATIONS

Ana Paula Oliveira | Summer Walker

MARCH 2024

ACKNOWLEDGEMENTS

The authors would like to thank Ian Tennant for his feedback as well as the Global Initiative Against Transnational Organized Crime (GI-TOC)'s Publications and Communications teams.

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.

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.

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

www.globalinitiative.net

Contents

SUMMARY

The attempt by the United Nations (UN) to develop a treaty to address cybercrime – or crimes committed online – has been put on pause. At the February 2024 concluding session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (henceforth 'AHC') in New York, member states were unable to reach agreement on several substantial issues. A final draft of the treaty therefore cannot be implemented – for now – and the process is on hold.

The issues on which states have not been able to agree after two years of negotiations have left a large question mark over what this convention, or potential convention, fundamentally entails. They include critical unanswered questions, such as the treaty's scope for preventative measures; the scope for collecting electronic evidence; the question of how human rights and legal safeguards would be protected were the treaty to be enacted; and what kinds of legal activities would be criminalized under its terms. The disagreements over these core components hinged on what types of government intervention – and interference – would be sanctioned by this treaty were it to be adopted. For example, would it allow states to criminalize certain activities that fall beyond the scope of what is 'normally' considered to an act of cybercrime, such as ransomware attacks? Could it become, for example, a legal instrument to suppress online dissent?

So, while delegates from all over the world have worked together to come up with a draft a treaty, line by line over the last two years, decisions to determine critical language – and function – of the treaty could not be made. For this reason, the negotiations have been put on hold until possibly July 2024, and maybe even later. At this stage, there are three possible scenarios:

- The first is that funding and UN General Assembly approval are secured for another meeting in July 2024 (or perhaps earlier). If so, delegates would in the meantime work to find consensus, so that at that meeting they would be able to adopt a treaty.
- The second is that funding or agreement is not secured within the UN to continue the process, or governments delay the approval of funds as a political tactic to stall the overall process, and the process gets shelved, meaning there would be no final treaty.
- The third scenario is that a country or group of countries bypass the AHC process and bring a draft to a vote at the General Assembly. This would mean a simple majority would be needed to approve a treaty, and it is unclear which way that vote would go.

This paper analyzes the sticking points that remain, namely the scope of the convention, the extent of human rights protections and the scope for international cooperation on electronic evidence, and assesses the challenge of moving forward with the treaty.

BACKGROUND

After two years of negotiations, governments gathered at the UN in New York from 29 January to 9 February 2024 for the final session of the AHC. Failing to reach agreement on key issues needed to finalize a treaty, the committee decided to suspend the session and reconvene later this year, depending on approval by the UN General Assembly and availability of resources. The latter is an important condition, given the UN's current liquidity crisis and the fact each AHC meeting costs about US$1million.[1] As mentioned in GI-TOC coverage of the treaty negotiations, the response from the General Assembly and the committee of delegates dealing with the budget will reflect the level of political importance that states attach to the process.[2]

The political divide that has characterized the previous six meetings[3] continued to set the tone for February's negotiations. The AHC worked in two streams, trying to reach agreement on the wording and terms of the treaty in the plenary, while addressing the thorniest issues in 'informal' negotiations outside of the main room – without observers from civil society and the private sector being present. Progress in the first week was slow, and doubts about the very future of the process started to emerge.[4] While major issues were still being discussed behind closed doors, the plenary moved to discuss what should be in the accompanying resolution that would be submitted for approval to the General Assembly with the future treaty. To debate the resolution that would give birth to a convention that did not yet even exist was a surprising use of the plenary's time.

In the second week, the Chair proposed a compromise package to the plenary, which had been discussed in the informal sessions. This included provisions on the core issues on which member states had not yet reached agreement, namely human rights safeguards, the scope of the convention and international cooperation. However, during the final days of the proceedings it was evident that substantive progress was not being made. The disagreements stuck, often exposing the diverging cultural and social values that countries have brought to these negotiations since the start. Some countries even recommended inserting entire new articles, making the committee redirect and address these additions. At that stage, there was simply not enough time or political capital left to reach the necessary compromises[5] and ultimately the delegates could not overcome the substantial divisions that have plagued the discussions from the beginning.

What's in a name?

Down to the very name of the treaty, two competing visions for this convention have not been reconciled during the AHC's two years of negotiations. The first option, favoured by one set of states, envisions a cybercrime treaty to address cyber-dependent crimes; the second is a treaty that addresses crimes committed using ICT. There is a vast, and now seemingly insurmountable, chasm between the two.

In the case of the former, a global treaty that addresses cybercrimes models itself on the Council of Europe's Budapest Convention. The ultimate aim of this type of treaty would be to combat crimes that can be committed only through the use of information and communications technology (ICT) devices, though governments advocating for this kind of treaty have allowed for the inclusion of tech-facilitated fraud and offences related to child sexual abuse material (CSAM) – in other words, extending its scope to certain cyber-enabled crimes. Those advocating for this type of treaty have generally also been open to including cooperation on electronic evidence on a wider set of crimes.

The question then is, why is there a need for another treaty that would in many respects duplicate an existing one? The answer is that the Budapest Convention is regional, and it needs to be recalibrated for a global context.

This is essentially what the current process has worked to do, borrowing language from the Budapest Convention, as well as UN criminal justice treaties such as the United Nations Convention Against Corruption (UNCAC) and the United Nations Convention Against Transnational Organized Crime (UNTOC). Budapest, drafted 20 years ago, also contains provisions that some in civil society have cautioned are too flexible for a global treaty, such as on the collection of electronic evidence.[6] Voices in civil society circles have seen this as an opportunity to align the cybercrime treaty with current knowledge and best practices. This is especially pertinent in the context of the values that Council of Europe members sign up to on issues like human rights and the rule of law. Given the transnational (and transcontinental) nature of cybercrime (e.g. ransomware attacks), a cyber-dependent treaty at the UN would provide a suitable forum for discussing and combating these evolving challenges with a wider group than Budapest Convention members.

The second vision is of a treaty that addresses crimes committed using ICT, which in a draft submitted by Russia at the beginning of the process in 2022[7] encompasses cooperation on essentially any type of crime if committed using ICT. While this conceptualization of the treaty includes cyber-dependent crimes, it would also include most existing forms of crimes if committed using information technology. Many were concerned that this approach would sanction government repression online and increase authorities' surveillance and monitoring powers, such as collecting data from a service provider without due process.[8] In addition to these serious concerns over the infringement of rights and liberties, a wide-ranging treaty of this nature raises the issue of how all of its actions would actually be implemented – for example, where would you prioritize resources and funding? And the question remains, what would be implemented through such a treaty that could not be implemented by other treaties through a resolution addressing technology? Why would a treaty for crimes through ICT differ greatly from ones addressing existing protocols, such as the mutual legal assistance treaty (MLAT) system outlined by the UNTOC and other regional and bilateral treaties? If the existing system were to simply encompass requests for electronic evidence, would this not satisfy the basic need of this treaty? Will the cooperation system it sets up (a 24/7 mechanism to manage mutual legal assistance requests) be exhausted by the number of requests and create a backlog worse that what we have today? There are limitations for any treaty implementation body, so consideration of what needs are most critical would support better implementation.

Disagreements over the title – and thus the fundamental purpose of the treaty – reigned during the last AHC session. With states unable to reach common ground, there was no prospect of being able to work through the detail.

These issues, discussed in more detail below, are representative of the debate that has dominated the process on the kinds of wide-ranging state powers this treaty would legitimise, and legalize, were it to be adopted. These are the overall scope of the convention; the collection of electronic evidence; human rights and legal safeguards; and the scope provided in the treaty for states to take criminal action against certain activities. Most of these were addressed in the Chair's compromise package, which in the end was not enough to bring the divergent sides together.

THE STICKING POINTS

Scope

The scope of a convention provides the parameters for what the parties can, and cannot, achieve through its implementation. The objectives of the treaty are set out in its scope provision. However, the lack of agreement on the purpose of the treaty made it impracticable to agree on the language to be used in such a provision.

WHAT IS CURRENTLY IN THE SCOPE?

The proposed text to Article 3 in the Chair's latest compromise document states that the Convention has a dual propose:

1. To prevent, investigate, and prosecute criminal offences established in accordance with this Convention – this gives states the ability to take criminal action to tackle the crimes listed in the Convention, which are currently a list of cyber-dependent crimes and some cyber-enabled crimes.
2. To collect, obtain, preserve and share electronic evidence for the purpose of criminal investigations or proceedings – here the Convention authorizes states to cooperate on electronic evidence on crimes beyond those cybercrimes outlined in the Convention that [may or may not be] cyber-related.

This duality on scope is at the core of many of the other issues that emerged throughout the AHC process. The reason for expanding the scope of cooperation on electronic evidence is to accommodate the needs of member states that want to prosecute crimes, even if committed in the physical, offline world but for which evidence can only be obtained in electronic form. This may include, for example, capturing a conversation on social media that contains evidence of a murder or footage of a shooting stored in the cloud.

While collecting electronic evidence is indeed critical, in a global treaty this provision has to be weighed against the need to ensure privacy is protected in the transmission of data and in replying to requests from state authorities. This necessitates a consideration of limitations, such as what would warrant a valid request for electronic evidence. Articles in the treaty should identify and address shortfalls in the current system by considering what cooperation needs are not being met by the current international cooperation system. If it is a question of speeding up processes, then for governments to be able to use the operational system (the 24/7 network[9]) to request data would be unlikely solve the problem, and could indeed create more delays. Besides, by expanding the scope, an opportunity for misuse of the instrument arises. By arguing that collecting e-evidence is essential for criminal prosecution, states could in theory abuse access to personal information to harass minority groups, opposition parties, journalists and others.

To mitigate these risks, Canada proposed an addition to Article 3. This proposal is designed as a safeguard to prevent the convention from being manipulated to persecute individuals and prevent it from being interpreted in a way that would be inconsistent with the obligations and responsibilities binding upon member states to protect the rights of individuals.

CANADA'S PROPOSAL

Nothing in this Convention shall be interpreted as permitting or facilitating repression of expression, conscience, opinion, belief, peaceful assembly or association; or permitting or facilitating discrimination or persecution based on individual characteristics.[10]

Member states opposing this provision argue that the wording proposed by Canada lacks a legal basis and precedent. The compromise presented in the Chair's package includes a new article, which that partly reflects Canada's proposal and moves the item from the scope to the implementation chapter of the convention text. Despite the welcome reference to human rights, the difference in language and position in the text deprives Canada's proposal of its intended political weight.

CHAIR'S PROPOSAL

59.3. Nothing in this Convention shall be interpreted as permitting or facilitating unlawful restrictions on human rights and fundamental freedoms, in accordance with applicable international human rights conventions.[11]

The dual scope of the treaty meant member states expended more energy on deflecting potential abuses than on tailoring the provisions on cooperation in obtaining evidence to combat cybercrime in line with the criminalization chapter. The discussions on scope represent a fundamental impasse that member states will have to resolve before any the other remaining sticking points can be addressed.

Human rights and legal safeguards

Aside from the safeguards discussed above, two other points on human rights in the general provisions are noteworthy.

The first is whether the treaty will contain a general provision on human rights, currently represented by Article 5 of a compromise package. This article, titled 'Respect for human rights', obliges states parties to ensure that implementation of the convention is in line with international human rights law. Although this article is supported by many member states, some expressed concern that a general human rights provision could 'interfere with the sovereignty and internal affairs of states'.[12]

This provision is an important measure, in that it aligns any future, potential cybercrime treaty with international human rights law. It reinforces human rights by placing them on an equal footing to security needs, meaning that human rights would be considered as guiding principles in the responses to organized crime, and not as an afterthought. It is critical that this is included in the general provisions chapter, where the rules of the treaty are set forth. This is in line with the approach taken in the Trafficking in Persons and Smuggling of Migrants Protocols to the UNTOC, which references human rights in its provisions. However, a reference to human rights in a single provision is far from enough: criminal justice safeguards, such as due process, should be underscored throughout the document.

The second question is whether Article 24 ('conditions and safeguards') should be strengthened. This article is pivotal to how human rights are envisioned in the treaty, in that it provides protection against abuse in the implementation of law enforcement. It sets out safeguards that can be invoked by individuals if the actions of law enforcement agents violate their rights during the course of an investigation or while deploying the intrusive

powers granted by the treaty. It provides citizens with the right to seek remedy and independent review, among others. However, the wording of this article has shortcomings. For example, there is no reference to transparency (i.e. the obligation to inform a person whose privacy has been restricted) and there is excessive emphasis on domestic law, which is a risk, as the potential states parties to this treaty have widely differing standards in respect to human rights.

Discussions on Articles 5 and 24 were mostly carried out in closed sessions, which were not open to civil society observers. Ultimately, states failed to reach consensus and both articles remained in the Chair's package of proposals.

The collection, storage and sharing of electronic evidence

A related sticking point is the scope of electronic evidence collection. In other words, for which crimes would states have the power to collect evidence in electronic form? There are two possible provisions set out in the treaty as it stands:

- Article 23.2c – intra-state collection on electronic evidence. This provision gives state agencies powers to collect evidence in electronic form for any criminal offence for the purpose of criminal investigations or proceedings. Such a criminal offence includes crimes that have no connection with cybercrime activity, but where evidence may exist in an electronic format.
- Article 35.1c – inter-state cooperation for collection on electronic evidence. This provision imposes on states the obligation to cooperate with other states to obtain electronic evidence for any serious crime, including serious crimes established in accordance with other applicable UN conventions and protocols in force at the time of adoption of this convention.

As can be seen in these articles, one of the options before the committee is therefore to include 'serious crimes' as a justification for international cooperation on collecting electronic evidence. This begs an important and concerning question: what is a 'serious crime'? Here, the definition of serious crimes is taken from the UNTOC (i.e. crimes that carry a minimum four-year penalty). This is problematic and contentious, as highlighted previously.[13] Effectively, under these terms the treaty would provide for the sharing of electronic evidence between two states for any offences that have a four-year penalty, qualifying them as 'serious crimes'. This means, for example, that if two countries consider homosexuality to be a crime punishable by a four-year sentence, they could use this convention to share electronic evidence, allowing for cross-border prosecution of individuals on the basis of their gender identity.

As member states could, once again, not agree on the language and in order to increase safeguards around human rights, a suggestion that seemed to gain traction (even with some 'middle ground' states) was the possible inclusion of Article 40, paragraph 20 bis to the draft convention.[14] This article revives New Zealand's proposal to provide states with an opt-out from cooperating (i.e. grounds for refusal). 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 if the scope remains broad by allowing for cooperation on any serious crime.

Criminalization

The debates on the criminalization chapter centred on whether it should include a wider or narrower range of crimes. This dividing line – polarizing the member states who favour a narrowly defined scope for criminalization and those who want a broad and ambiguous treaty – has characterized the AHC negotiations since the start. Representing the latter group, Russia expressed discontent during the 7th AHC for feeling ignored in its attempts to introduce more offences into the convention.

WHY THE CRIMINALIZATION CHAPTER MATTERS

- The criminalization chapter imposes obligations on states to make a certain activity a criminal act under their domestic laws. It sets out which activities are deemed illegal and for which perpetrators can be investigated, prosecuted and, if found guilty, sentenced.
- The criminalization chapter provides useful guidance for member states in shaping their domestic laws, bringing standardization and legal certainty. For example, the definitions of the phenomena included in the criminalization chapter in the UNTOC serve as the basis for a common global understanding of transnational organized crime, influencing national laws and international cooperation on criminal matters.
- Conversely, loosely defined criminalization may lead to excessively punitive state responses to crime and overcriminalization. Consequently, states might face other issues, such as overincarceration.
- Making something a criminal offence is not the answer to all problems. That is why CSOs have been arguing for a narrow scope of criminalization in this chapter to avoid the adoption of an overly punitive approach that criminalizes activities that should not be penalized or do not merit international cooperation.

In this respect, two provisions are still in play. One is Article 60 of the compromise package, which creates an obligation for member states to criminalize offences established in accordance with existing UN conventions and protocols – if such offences are committed using ICT. This provision is a version of an earlier article in previous drafts, which attempted to ensure that offences established in accordance with any international conventions and protocols also apply when committed through the use of ICTs.[15] The difference in the new wording is that it mandates member states to criminalize offences as defined in the UNTOC, as opposed to any instrument existent in international law.

Secondly, there is a potential risk that the list of crimes covered by the convention would be expanded by the proposal Article 5bis of the draft resolution (to accompany the convention through its approval process at the General Assembly), proposed by Russia and not yet agreed by member states.[16] This proposed new paragraph would allow states to begin drafting a protocol to include further crimes that do not make it into this treaty. A protocol addressing additional forms of offences and relevant mechanisms, consistent with the scope and implementation of the convention, could be the subject of future negotiations by the AHC over the next year and a half (i.e. before this treaty potentially enters into force). Given that the scope of the convention has not yet been defined, it is not surprising that this idea was quickly dismissed by the US and others. The concept itself is dangerous, as a group of member states not party to the convention could potentially negotiate a protocol to it.

Two provisions of this chapter that were key for many member states and civil society groups seemed to be heading nowhere towards consensus – namely, the articles on online sexual abuse (Article 13) and non-consensual distribution of intimate images (Article 15), as discussed below.

Provisions related to the protection of children and images

One of the challenges faced by delegates relates to online child sexual abuse or child sexual exploitation material (Article 13). Two main points of discussions were:

- Legal implications of the term 'without right'. This wording seeks to safeguard those who may be in possession of such material but had no intention of committing the offence, for example a person who has been trusted with the material by the victim. If this wording is retained, a person could be prosecuted only if they possess abusive material 'without right' to do so.
- Deletions of paragraphs 3 and 5 from Article 13. These paragraphs include safeguards to prevent the criminalization of children who engage in consensual relationships and to ensure protection of privacy. The deletion of the provisions was strongly opposed by Jamaica (on behalf of the Caribbean Community), Liechtenstein, Argentina, Norway, Australia, Japan, Uganda, Iceland, Switzerland, Vanuatu, Georgia, Austria, the UK, New Zealand and the EU, considering the detrimental effect of potentially criminalizing teenagers who voluntary share images with partners. The deletion was supported by Egypt, Iran, Oman, Libya, Syria, Qatar, Sudan, Cameroon and other countries.

A second point of contention on these issues relates to Article 15 and whether intent should be maintained as a requirement of the offence. This means that if the dissemination of the material were authorized by the person who is depicted in the material the conduct would not be a criminal offence. Without considering the victim's consent, the convention would thus risk criminalizing the very victims it seeks to protect. By striking off intent, there is a risk of over-criminalizing women in countries where pornography is a criminal offence. Canada, for example, said that a provision designed to protect privacy could instead turn the issue into a 'moral offence'.

The statements in relation to these articles laid bare the gap between cultural and social principles espoused by Western countries and the predominantly Arab group (working closely with Iran), representing fundamental differences of opinion that seem difficult to bridge if the meeting resumes.

Technical assistance

Many of the articles in the chapter on capacity building and technical assistance were agreed to in the concluding session. However, the issue of the nature of technical assistance continued to divide the AHC, in particular Article 54(1), which imposes on states the duty to provide assistance to one another in accordance with their capacity, in the form of training, exchange of experience and specialized knowledge, and transfer of technology.[17] Technological transfer is an important goal in technical assistance to developing countries. While some member states (many of them developing countries) would prefer a draft that reflects the mandatory nature of the provision of technical assistance, others (many of the Western countries) would rather downplay the expectation of technology transfer through the convention.

Preventative measures

Another important provision of the draft, which states have not agreed on is contained in Article 53(3) in the chapter on preventative measures. This is a chapter that contains provisions related to the prevention of cybercrime. The sticking point here is a terminological dispute over the term 'gender-based violence'. The Chair's draft emphasizes the need to develop strategies and policies to prevent and eradicate gender-based violence. This is a key provision to protect the needs of people who, because of their gender, are disproportionately affected by the crimes committed through the internet.

CONCLUSION

The future of the treaty process now hinges on several bureaucratic and political factors. Funding for the next meeting has to be requested through the 5th Committee of the UN and approved. It is unclear if this can be achieved before July and whether rooms can be booked during the busy July schedule when other major events take place at the UN headquarters. There will also have to be time and budget allocated to interim meetings for governments in Vienna ahead of a next AHC meeting, during which states would try once again to bridge the seemingly irreconcilable differences that have plagued the process since the beginning and continue to divide state positions on this treaty. Given these uncertainties and bureaucratic obstacles, the AHC could either succeed in adopting a treaty later this year, or face delays or further disruption.

It is now up to the member states to decide what type of treaty they want, and therefore which direction the treaty process will go. At the moment, the draft faces an uphill battle before it can be adopted by consensus by governments at the UN.

Notes

[1] Darren Brookbanks and Ana Paula Oliveira, A dream deferred or a near miss? UN committee postpones decision on cybercrime convention, GI-TOC, 15 February 2024, https://globalinitiative.net/analysis/un-committee-postpones-decision-cybercrime-convention.
[2] Ibid.
[3] Ian Tennant, The cost of consensus: Sixth session of the UN Ad Hoc Committee on cybercrime, GI-TOC, 14 September 2023, https://globalinitiative.net/analysis/united-nations-cybercrime-treaty-negotiations.
[4] See Cyber Convention Check-in, GI-TOC, 26 January to 9 February 2024, https://globalinitiative.net/announcements/cyber-convention-check-in.
[5] Darren Brookbanks and Ana Paula Oliveira, A dream deferred or a near miss? UN committee postpones decision on cybercrime convention, GI-TOC, 15 February 2024, https://globalinitiative.net/analysis/un-committee-postpones-decision-cybercrime-convention.
[6] Deborah Brown, Cybercrime is dangerous, but a new UN treaty could be worse for rights, Human Rights Watch, 13 August 2021, https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights.
[7] Unofficial Draft, 29 June 2021, United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes; https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.
[8] Rishi Iyengar, Robbie Gramer and Anusha Rathi, Russia is commandeering the U.N. Cybercrime Treaty, Foreign Policy, 31 August 2023, https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty.
[9] The 24/7 network would have a designated point of contact available 24 hours a day, seven days a week, in order to ensure the provision of immediate assistance for the purpose of international cooperation.
[10] 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.
[11] See Chair's proposal on articles 3, 5, 17, 24 and 35, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Documents/2402464E.pdf.
[12] Egypt statement, on behalf of the Arab Group, supported by Pakistan, Russia, Iran and Iraq.
[13] See Ian Tennant, Endgame: The final phase of the UN cybercrime negotiations?, GI-TOC, January 2024, https://globalinitiative.net/analysis/united-nations-cybercrime-negotiations-final-phase.
[14] This proposal was supported by the EU, Brazil, Argentina, Uruguay, Canada, Chile, the US, Liechtenstein, Mexico, Peru, Singapore, Sweden, Norway, Iceland, Colombia, Georgia, Japan, Albania, Costa Rica, Australia, Kiribati, Vanuatu and Moldova. It was not supported by Egypt, Cuba, Mauritania, Iraq, Oman, Burkina Faso, Libya, Tanzania, Namibia and Bahrain.
[15] Summer Walker, Closing Pandora's box: UN cybercrime treaty negotiations, GI-TOC, August 2023, https://globalinitiative.net/analysis/un-cybercrime-treaty-negotiations-august-2023.
[16] See Draft resolution for consideration by the General Assembly, UN General Assembly, https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FAC.291%2F25&Language=E&DeviceType=Desktop&LangRequested=False.
[17] One of the changes proposed by the US (supported by Norway, Switzerland and others) in that regard was to add the words 'voluntary' and 'mutually agreed terms' to reflect the fact that technical assistance is based on mutual agreement between the recipient and donor states. In the end, the US withdrew from the proposal for the sake of consensus, which appeared to be a considerable compromise. However, Iran tried to push further by proposing to delete the caveat 'where possible' from Article 54.1, and the provision was not agreed in plenary.

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