GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ENDGAME

THE FINAL PHASE OF THE UN CYBERCRIME NEGOTIATIONS?

Ian Tennant

JANUARY 2024

NOTE

This brief is produced ahead of the 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, 29 January–9 February 2024, New York.

ACKNOWLEDGEMENTS

The author would like to thank Ana Paula Oliveira for her research and insights, as well as Elsadig MohamedAhmed for his feedback.

This policy brief was supported by the United Kingdom's Foreign, Commonwealth and Development Office (FCDO). The views expressed do not necessarily reflect the views of the United Kingdom FCDO.

ABOUT THE AUTHOR

Ian Tennant is based in Vienna, where he leads the Global Initiative Against Transnational Organized Crime (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.

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

www.globalinitiative.net

CONTENTS

THE CONTEXT **2**

The different camps 3

THE NEW DRAFT: AN AUTHORITARIAN'S DREAM **4**

THE PROCESS AT THE FINAL SESSION **9**

THE CONCLUDING SESSION: POSSIBLE OUTCOMES **10**

Notes 13

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

FROM VISION TO ACTION: A DECADE OF ANALYSIS, DISRUPTION AND RESILIENCE

The Global Initiative Against Transnational Organized Crime was founded in 2013. Its vision was to mobilize a global strategic approach to tackling organized crime by strengthening political commitment to address the challenge, building the analytical evidence base on organized crime, disrupting criminal economies and developing networks of resilience in affected communities. Ten years on, the threat of organized crime is greater than ever before and it is critical that we continue to take action by building a coordinated global response to meet the challenge.

THE CONTEXT

From 29 January to 9 February 2024, delegates will gather at the UN headquarters in New York for the 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, the AHC). Over the past two years, the AHC has held six sessions to draft a new UN convention on cybercrime. But so far, in increasingly difficult geopolitical times, delegates have failed to reach consensus on any of the key issues the AHC was tasked to address.

As the Global Initiative Against Transnational Organized Crime (GI-TOC) has documented,[1] there is a wide range of views among AHC delegates about the very purpose of this treaty, what crimes it should address, what states should be empowered to do in response, and what safeguards should be put in place to protect human rights and freedom of speech. Even the name of the convention has yet to be decided.

The AHC began its work in the aftermath of the Russian invasion of Ukraine in 2022, and statements about it have overshadowed the proceedings throughout, particularly as Russia – as a long-time advocate of a UN cybercrime treaty and an opponent of the idea that more states should sign up to the existing Council of Europe Budapest Convention – tabled the resolution that launched the process and submitted a full draft treaty.[2] As the concluding session approaches, the state of multilateralism has deteriorated in the context of the Israel–Hamas war and we can expect this to cast its shadow over the proceedings. In this context, the AHC, chaired by the Algerian diplomat Faouzia Mebarki, is mandated to produce a draft text.

It is worth recalling that the polarization of views on a potential cybercrime treaty pre-dates the current fragile state of multilateral diplomacy. After a 2010 UN Crime Congress declaration first floated the idea of such a treaty,[3] a 2013 draft study by the UN Office on Drugs and Crime (UNODC) exploring the possibility[4] was never officially adopted because it recommended pursuing a new convention[5] – an idea rejected by the pro-Budapest Convention group of mainly Western countries.

Throughout this period of political stalemate, the complexity and pace of technological advancement have continued to benefit cybercriminals of all kinds, who have consistently used it to their advantage to open new markets, and diversify and expand their operations and profits, often at the expense of the most vulnerable in society. And their success has often been linked to the acquiescence or even collaboration of some states.

> *Since 2000, the 'great accelerator' – new technologies, including information communications technology (ICT) – has supercharged illicit markets by improving operations and covert communications, increasing crime groups' adaptability to enforcement measures and expanding the size and diversity of both groups and markets. In the process, the criminal underworld has become seamlessly joined with the upperworlds of business and politics, blurring distinctions between illegal and legal.*
>
> – GI-TOC, The global illicit economy[6]

During the same timeframe, views on the nature of internet governance and digital rights have continued to diverge.[7] All governments take advantage of the data the internet has given them to pursue bad actors, but the range of human rights protections, rule of law and judicial oversight on how that data is used or shared varies enormously. And in some places, the ability to control and monitor populations through the internet offers irresistible advantages.[8]

Indeed, 'cybercrime' legislation itself is often used as a tool for control and repression, as any activity deemed as 'criminal' that takes place online can be classified by authorities as a form of 'cybercrime'.[9] As GI-TOC reports have previously highlighted, there is no 'digital rights' treaty to protect against this nefarious use of cybercrime legislation.[10]

That is why these negotiations are fundamental to the future of the internet, human rights and digital freedoms, and indeed the future of multilateralism. There is a real risk that a new treaty will call into question the role of the UN in relation to human rights, and could herald a new era in which the UN can be shaped by small groups of states to be used as a tool and justification for surveillance and repression, rather than as a guarantor of the universal values of human rights, peace, security and justice forged in the aftermath of World War II.[11]

The different camps

There is one camp of countries, led by Russia and China, that would like to use these negotiations to advance their vision of a tightly controlled internet where a broad and ambiguously defined range of activities can be outlawed at the international level with a UN stamp of approval,[12] and where countries are empowered to share information and engage in 'international cooperation' to prosecute and extradite individuals deemed to have committed 'cybercrime', and to extract data and information from those who hold it (i.e. the private sector service providers based in the West).[13]

At the other end of the spectrum, a small group of countries, primarily Canada and New Zealand, understand the threat to universal values embodied by the UN that this approach poses and have consistently advocated for a treaty that explicitly safeguards against such actions.[14]

In between these two ends of the spectrum are several groups of states. Close to Canada and New Zealand are the US, the UK, the EU and most other Western and Latin American countries, as well as Asian states, such as the Philippines and Thailand, and African countries, such as Nigeria and Ghana, which maintain strong positions on human rights and safeguards, but have conceded that the exchange of 'e-evidence' on a wide range of crimes could be accepted under the treaty, which they believe poses less risk to rights and freedoms.[15]

Russia and China are joined by a small group of vociferous supporters, including Nicaragua, Burundi, Mali, Eritrea and Tajikistan. Closer to the centre of the spectrum, however, is a broad group of countries (with varying positions) that generally want to ensure that the treaty provides them with access to wide-ranging opportunities for cooperation, capacity building and technical assistance (including technology transfer). Key players in this group include the Caribbean Community (usually represented by Jamaica), which has maintained a surprisingly hard line against human rights safeguards; Brazil, South Africa and India, which have supported China and Russia in advocating for a treaty (as a shared BRICS priority); and others, including Egypt, Singapore, Pakistan and Yemen – all generally supportive of a broad treaty, but with different focuses, such as specific crimes they would like to be included, and a general reluctance to see an expansive set of human rights safeguards, which they characterize as an obstacle to the treaty's effectiveness.

Positions have not changed throughout the negotiations and movement towards agreement has been the exception, not the rule.[16] A zero draft was presented and debated at the AHC's sixth session in New York in August–September 2023.[17] The AHC has not met formally since then, but informal discussions are now taking place more regularly in Vienna. In late November 2023, delegates finally received the draft convention to be considered at the AHC's upcoming final session in January–February 2024. For those following the process with concern about where it might lead, the new draft made for uncomfortable reading.[18]

THE NEW DRAFT: AN AUTHORITARIAN'S DREAM

The draft, published in November 2023,[19] is the second official draft text produced by the AHC Chair, following the 'zero draft' published in the run-up to the sixth session in mid-2023.[20] The new and essentially final attempt at a draft has many similarities to that earlier draft, which the Chair concluded was the best way to achieve consensus, despite the lack of progress at the sixth session.[21]

The new draft follows the same structure as laid out in the AHC sessions and the 'zero draft', and therefore retains strong influence from existing instruments such as the UN Convention against Transnational Organized Crime (UNTOC), the UN Convention Against Corruption and the Budapest Convention. However, the points of contention remain in italics – i.e., the Chair has decided not to propose a solution to the main sticking points, but rather to leave it to the delegates to come to an agreement on them before or during the concluding session. The 'Note by the Chair' accompanying the draft states that 'with regard to the provisions on which views appear to be the most divergent, the Chair preferred not to present a new compromise proposal at this stage, in order to allow for the continuation of bilateral and open-ended informal discussions.'[22]

However, some sections have also removed references that limit the application of the convention to the offences listed in Articles 6–16, meaning that the new text moves away from a limited scope to a much broader and more ambiguous treaty – and one that poses more risks to rights and freedoms than the zero draft. This approach demonstrates the lack of consensus on key points of the text and ignores the view of most observers of the process: that the zero draft itself was too broad. The changes in the new version of the text are analyzed below:

- Article 2 (Use of terms). This is the section that outlines the definitions of technology – for example, whether to refer to a 'computer system', as preferred by Western countries, or the more ambiguous 'information and communications technology device', as proposed by Russia and its allies. Similarly, the choice between the clearer 'computer data' or the more vague 'digital information'.

  This section also includes the misleading UNTOC definition of 'serious crime' as 'an offence punishable by a maximum deprivation of liberty of at least four years'.[23] This definition is one of the means by which this convention could enable a wide range of government abuses, without the broader context of cooperation included in the UNTOC.

- Article 3 (Scope of application). This article, which is unchanged from the zero draft, states that the convention will apply to the 'prevention, investigation and prosecution of the offences established in accordance with this convention, including the freezing, seizure, confiscation and return of the proceeds of such offences'.[24] The zero draft's reference to Articles 6–16 is maintained, but other parts of the text keep the convention open to the vague offences referenced elsewhere in the text.

  This article also states that the convention will apply to the 'collecting, obtaining, preserving and sharing of evidence in electronic form, as provided for in the relevant articles of the convention'.[25] This is another worrying provision that, when combined with other articles, could allow for the sharing of electronic evidence for an endless list of 'crimes'.

- Article 5 (Respect for human rights). This article should serve as an overarching safeguard for the application of the whole treaty. This has been denoted in the new draft as not being agreed, although agreement has been reached on Article 4 (protection of sovereignty), which guarantees states' rights. This is a welcome and necessary provision, but it needs to be strengthened, for example by naming the principles and rights that should guide the interpretation of the Convention (such as proportionality, necessity and legality).

  A Canadian proposal, which was submitted at the sixth session and would provide a more holistic and stronger human rights safeguard, offers the following language: 'Nothing in this Convention or its interpretation or application by States shall permit or facilitate repression or suppression of expression, conscience, opinion, belief, assembly or association; or permit or facilitate discrimination or persecution based on personal characteristics.'[26]

- Article 24 (Conditions and safeguards). This article, related to Chapter IV (Procedural measures and law enforcement) outlines in point 1 that the procedural measures and law enforcement powers included in the treaty are 'subject to conditions and safeguards provided for under its domestic law, which shall be consistent with its obligations under international human rights law, and which shall incorporate the principle of proportionality'.[27] This could be strengthened by adding references to necessity, legality and protection of privacy and personal data in addition to proportionality.

  Judicial oversight is also key to prevent abuses of power, as is the right to challenge government requests for data. The GI-TOC believes that judicial review should therefore be retained in Article 24(2) and strengthened by removing the 'as appropriate' caveat in its application. In addition, references to transparency and accountability should be included in 24(2), alongside the existing measures proposed. Taken together, these references reinforce the legal safeguards for procedural measures by providing certainty and increasing the level of legitimacy and checks and balances in the decision-making process.

  Furthermore, Article 24's application should be broader than just for Chapter IV, for example by moving this provision to Chapter I (General Provisions) to ensure that it also applies to Chapter V.

- Article 35 (General principles of international cooperation). This article outlines the scope of international cooperation in the convention. It says that states:

  > shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable instruments on international cooperation in criminal matters, and domestic laws [...] concerning offences established in accordance with this convention, or for the collection, obtaining, preservation and sharing of evidence in electronic form of offences established in accordance with this convention, as well as of serious crime, including those offences covered by Article 17.[28]

Crucially, the reference to Articles 6–16 have been removed as compared to the zero draft. This means that the provisions can be applied to all offences in this treaty, any other relevant treaty, national law and any 'serious crime' (meaning an offence punishable by imprisonment of four years or more). This is an incredibly broad scope for international cooperation, and an even broader scope for the sharing of electronic evidence – which can take place in relation to any offence that qualifies as a 'serious crime'. This means, for example, that if two countries consider homosexuality to be a serious crime, they could use this convention to share 'electronic evidence'.

As it stands, the new draft reads even more like a convention that allows for unfettered surveillance and state harassment than a treaty that ensures a more effective international response to cybercrime. This lack of clarity and broadened scope, and therefore increased risk, is exacerbated by the proposed Article 23(2), which states that the procedural and law enforcement powers of the convention will apply to the following levels of offence:

- The criminal offences established in the convention (again, the reference to Articles 6–16 has been removed)
- Other criminal offences committed through either a 'computer system' or an 'ICT device'
- The collection of electronic evidence on 'any criminal offence'

This article creates a very broad scope for the convention in terms of the 'offences' that could fall under it. The powers conferred by the treaty and the safeguards proposed are shown in Figure 1.

OFFENCES	DEFINED OR NOT?	POWERS IN THE CONVENTION	SAFEGUARDS AND GUARANTEES
INCLUDED IN CHAPTER IV (PROCEDURAL MEASURES AND LAW ENFORCEMENT)			
Acts criminalized in accordance with the Convention	Not clearly defined	All included in Chapter IV (including expedited preservation of data, disclosure of traffic data, search and seizure, production orders, interception of content data, etc.)	Article 5 (human rights catch-all provision) and all included in Chapter IV (including on conditions and safeguards, protection of witness and victim assistance and protection)
Other criminal offences committed by use of computer/ICT	Not clearly defined	All included in Chapter IV (including expedited preservation of data, disclosure of traffic data, search and seizure, production orders, interception of content data, etc.)	Article 5 (human rights catch-all provision) and all included in Chapter IV (including on conditions and safeguards, protection of witness and victim assistance and protection)
Any criminal offence	Not clearly defined	All included in Chapter IV (including expedited preservation of data, disclosure of traffic data, search and seizure, production orders, interception of content data, etc.)	Article 5 (human rights catch-all provision) and all included in Chapter IV (including on conditions and safeguards, protection of witness and victim assistance and protection)

OFFENCES	DEFINED OR NOT?	POWERS IN THE CONVENTION	SAFEGUARDS AND GUARANTEES
INCLUDED IN CHAPTER V (INTERNATIONAL COOPERATION)			
Acts criminalized in accordance with the Convention	Not clearly defined	All included in Chapter V (including extradition, MLA, preservation and disclosure of data, real-time collection of traffic data, etc.)	Article 5 (human rights catch-all provision) and all included in Chapter V (including dual criminality and grounds for refusal)
Serious crime	Not clearly defined	All included in Chapter V (including extradition, MLA, preservation and disclosure of data, real-time collection of traffic data, etc.) for the collection, obtaining, preservation and sharing of e-evidence	Article 5 (human rights catch-all provision) and all included in Chapter V (including dual criminality and grounds for refusal)

OFFENCES	DEFINED OR NOT?	POWERS IN THE CONVENTION	SAFEGUARDS AND GUARANTEES
INCLUDED IN CHAPTER VI (PREVENTION)			
Acts criminalized in accordance with the Convention	Not clearly defined	All included in Chapter VI (including strengthening cooperation between law enforcement, public awareness campaigns, capacity building of criminal justice systems)	Article 5 (human rights catch-all provision)

OFFENCES	DEFINED OR NOT?	POWERS IN THE CONVENTION	SAFEGUARDS AND GUARANTEES
INCLUDED IN CHAPTER VII (TECHNICAL ASSISTANCE AND INFORMATION EXCHANGE)			
Acts criminalized in accordance with the Convention	Not clearly defined	All included in Chapter VII (including training and other forms of assistance, exchange of experience, transfer of technology)	Article 5 (human rights catch-all provision)

FIGURE 1 Powers conferred by the treaty and the safeguards proposed.

Compared to the zero draft, the vague and open-ended scope of offences to be covered, which was already problematic,[29] is even more open to negative application or abuse due to the removal, in several places, of a reference to Articles 6–16 of the convention under the chapters covering procedural measures and law enforcement, and international cooperation, as well as the vagueness of Article 17, which could include offences agreed under regional conventions. The zero draft's references to Articles 6–16 provided some built-in (though insufficient) safeguards, and now that those references have been removed, there is even greater need for stronger safeguards for the treaty as a whole, and for Chapters IV and V in particular.

WHY STRONGER SAFEGUARDS ARE NEEDED

Dual criminality and grounds for refusal alone are not enough

It has been argued that a dual criminality requirement and grounds for refusal in extradition and mutual legal assistance (MLA) requests are sufficient to ensure that human rights safeguards are upheld. This serves the purpose of allowing states receiving requests to judge each one on its merits and to refuse cooperation if they believe that their human rights obligations would be undermined or if there is no dual criminality. However, the grounds for refusal must be accompanied by strong overarching safeguards.

Under the current draft, two states that have a similar law criminalizing, for example, acts that criticize the government or promote LGBTQIA+ identities, which could be considered crimes under the convention, could launch joint investigations, extradition proceedings or other MLA procedures. This would allow repressive states to work together under the UN flag to hunt down and share information about dissidents, critics or anyone they see as a challenge to their authority or religious or social values.

The 'serious crimes' threshold from the UNTOC cannot be used in isolation, and the collection and sharing of electronic evidence for a broad set of crime presents risks

The four-year imprisonment threshold comes from the UNTOC, which includes it as part of its set of requirements for international cooperation under that treaty. In addition to the 'serious crimes' threshold, the activities under investigation must be transnational in nature and carried out by a structured criminal group.[30] The other two conditions are not included in this new treaty. As currently drafted, governments are empowered to collect, store and share 'electronic evidence' of any serious crime, whether cyber-related or not. This means that an endless list of 'offences' could be subject to the treaty's powers – many of which are legal in other countries and even protected under international human rights law. It is not only 'serious crimes' that fall under the convention's remit of sharing electronic evidence. Chapter IV refers to 'any criminal offence' – including expansive powers on the collection, interception and preservation of data.

This would enable repressive states to justify their surveillance and investigation regimes as endorsed and supported by the UN.

THE PROCESS AT THE FINAL SESSION

According to its mandate, as set out in UN General Assembly Resolution 75/282,[31] Figure 2 shows what is expected of the AHC, including at its last session, cross-referenced with progress to date:

MANDATE AS SET OUT IN RESOLUTION 75/282	PROGRESS AND COMMENTS	COMPLETED
To hold six negotiating sessions in Vienna and New York	Completed, with no consensus achieved on any of the convention's main issues.	✓
To hold a concluding session in New York to be held 'for the purpose of adopting the draft convention'.	The session will take place from 29 January to 9 February 2024. The draft text prepared for the session leaves major issues unresolved, and states are still far from a consensus after six negotiating sessions.	
To 'conclude its work in order to provide a draft convention to the General Assembly at its seventy-eighth session'.	The 79th session of the UN General Assembly will open on 10 September 2024, with the 78th session closing shortly before. However, with the AHC's concluding session on 9 February, it must finish its work by then, as it will have no more resources or mandate to hold another meeting, unless member states decide otherwise.	
To make decisions by consensus as first preference, but with the ability to vote on substantive matters with a two-thirds majority required.	So far, no delegates nor the Chair have opted to call for a vote on the text or any part of it. If consensus is still not reached towards the end of the concluding session, we can expect a vote or a series of votes on the text or parts of it. The two-thirds majority means that proposals will need broad support to be adopted. However, votes on procedural issues are governed by UN General Assembly rules, meaning that a 50 per cent + 1 majority would be required. This rule could come into play if a decision on the future of the AHC is tabled.	
For the Chair to 'host intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention.'	The Chair has hosted five intersessional consultations with multistakeholders covering issues in broad alignment with the issues being discussed by the AHC.	✓
To 'take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.'	The draft text draws heavily on existing instruments. The work of the intergovernmental Expert Group (IEG) is less easily identifiable, but AHC delegates have access to IEG documentation and many delegates have participated in the IEG themselves.	✓
For member states 'to provide voluntary extrabudgetary financial contributions to the United Nations Office on Drugs and Crime to ensure funding to enable the participation of representatives of developing countries, especially those that do not have resident representation in Vienna, in the work of the Ad Hoc Committee, including by covering their travel costs and accommodation expenses.'	The UNODC has been able to support the travel and accommodation costs of some delegations/delegates. Member states also provide such support directly.	✓

FIGURE 2 The AHC's progress on its mandate.

THE CONCLUDING SESSION: POSSIBLE OUTCOMES

In December 2021, at the start of this process, the GI-TOC outlined four possible outcomes of an international convention on cybercrime:[32]

1. CONTROL: A new convention in line with the Russian draft.
2. CONTROL/ALT: A compromise convention.
3. ALT: The alter ego of the Budapest Convention.
4. DELETE: No result.

Based on what has happened thus far, all four outcomes are still technically possible. But now we would add a fifth possible outcome:

5. RELOAD: The AHC decides to extend its life or reinvent itself.

Below is an updated analysis of the likelihood and implication of each outcome:

1. CONTROL: A new convention in line with the Russian draft (or the revised draft). Given the low level of support for the extreme end of Russia's positions and the geopolitical reality, Russia's original vision of a treaty will not be adopted by consensus, considering the numbers required for a two-thirds majority. Although this type of treaty counts on the support of powerful countries such as China, it will not be adopted in this form either by consensus or by vote. However, a convention in the form of the revised draft could end up being acceptable to Russia, China and their allies, and would have a better chance of being adopted by vote if no compromise is reached.

2. CONTROL/ALT: A compromise convention. This is clearly the default option and what the resolution that mandated this process called for. However, the reality of the political issues and the disagreements on the text of the treaty also make this option a challenge. It is also the option that continues to raise alarm bells on rights and freedoms.

   The normal procedures of negotiation, including at the multilateral level, would dictate that when there are two opposing views, a consensus should be reached somewhere in the middle. However, in this case, the two extremes of the spectrum offer completely different worldviews and objectives for the negotiation. And when the negotiation is between (1) completely bulldozing human rights obligations and invoking the UN to subvert them in order to implement the treaty, and the opposite side of the spectrum, (2) maintaining the status quo, any movement towards position 1 is a major concession for those closer to position 2 and a significant win for those maintaining position 1.

   It remains to be seen how much of a win those in favour of position 1 are willing to take as a victory. That will come out in the concluding session. But it is highly unlikely that those countries seeking a broad convention will agree to both a narrow scope and the inclusion of the strong human rights safeguards that would be needed to maintain the status quo. The compromise that has gained the most traction so far is to allow broader cooperation or at least broader sharing of electronic evidence, with the UNTOC sentence threshold as a determinant of the offence that could be included in such a catch-all. However, even if limited

to electronic evidence sharing only, this opens the door to a UN treaty with a mandate to criminalize a range of activities that are not widely considered criminal and should be protected under international human rights obligations. A broader scope for criminalization and cooperation has repeatedly hit a dead end and seems unlikely to pass by consensus.

A more effective catch-all human rights safeguard (in addition to current Article 5), as proposed by Canada at the sixth session, could therefore hold the key to a consensus text, alongside a clear and defined scope of application and offences throughout the treaty. But it would need to be seriously scrutinized and tested to ensure that it applied to the whole convention and could not be ignored or circumvented. It would also have to pass the tests of the national systems that would need to adopt the legislation necessary to implement the convention at the national level. In any case, it would need to be acceptable to the likes of China and influential 'middle ground' countries such as Brazil, Egypt, India, South Africa and Pakistan to have a serious chance of success.

3. ALT: The alter ego of the Budapest Convention. One curious consequence of these UN negotiations has been increased interest in the Budapest Convention, with Nigeria formally acceding in 2022 and Tonga becoming a party in 2023. However, even among the Budapest parties, there is no consensus that the Budapest framework should be replicated for this convention. Human rights advocates have also highlighted the risks of this approach, given that the Budapest parties are mainly members of the Council of Europe and therefore aligned with its human rights and rule of law obligations. If the same provisions are applied to the entire UN membership, the same guarantees and trust needed for effective data sharing and international cooperation cannot be assumed.

   However, it is worth noting that if all the Budapest parties (68) plus the 23 countries invited to accede were to maintain a common position in favour of a Budapest-lite convention, 91 countries would be a strong number in any vote. However, it would still be less than 50% of the total UN membership, so much would depend on the number of countries present and voting to achieve a two-thirds majority in favour of such a convention.

4. DELETE: No result. This is the option that brings the most uncertainty. If the AHC's time runs out, it will cease to exist. It will have failed to fulfil its mandate, so the ball will go back to the UN General Assembly's court. States in favour of a particular position could submit a draft convention to be voted on at the General Assembly, which would only need a simple majority to be adopted, thus negating the work of the AHC. Perhaps two different conventions could be tabled, or resolutions calling for action to follow up on the committee. It could result in no action, or a new convention. It is understandable that diplomats are keen to avoid this scenario.

RELOAD: The Committee decides to extend its life or reinvent itself. To avoid the DELETE scenario, delegates could opt for another way out: either extending the life of the AHC or reinventing it. This would postpone the moment of final decision and try to find a new way of working for the AHC. This could, if there is a shared vision of the way forward and political will to reach a conclusion within a new timeframe, result in simply adding meetings and agreeing on a timeframe for a new concluding session to deliver its results before the end of a given General Assembly session.

This option would have the advantage of avoiding hasty decisions without the appropriate due diligence that has been undertaken in the negotiation of other conventions,[33] with lasting consequences, and allowing delegates more time to consider compromise proposals in more detail before reconvening with a clearer understanding of

the risks and opportunities of the more problematic and complicated issues. Such an outcome could include a commitment by all member states not to submit competing draft conventions directly to the General Assembly for the duration of the extended AHC, to ensure that only the AHC can produce a legal instrument. It could also secure the long-term participation of multistakeholders, as enshrined in the current AHC modalities, which has proven to be a useful and valuable exchange.

There is no question that a more effective international cooperation framework against cybercriminal activity would be beneficial. There are now two main questions for delegates:

- Is this this is the right way and the right time to do it?
- How much damage could be done and are there sufficient safeguards against potential risks?

NOTES

[1] See https://globalinitiative.net/initiatives/un-cyberwatch/.

[2] The draft treaty submitted by Russia was supported by China, Belarus, Burundi, Mali, Nicaragua and Tajikistan. See: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Russian_Fed_statement_-3rd_session.1.pdf.

[3] 'We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.' See Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World: https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

[4] UNODC, Comprehensive study on cybercrime, Draft, February 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[5] Ibid. See recommendation (f): 'The development of a comprehensive multilateral instrument on cybercrime, with a view to establishing an international approach in the areas of criminalization, procedural powers, jurisdiction, and international cooperation.'

[6] GI-TOC, The global illicit economy: Trajectories of transnational organized crime, 2021, https://globalinitiative.net/analysis/global-organized-crime/.

[7] Daniëlle Flonk, Markus Jachtenfuchs and Anke S. Obendiek, Authority conflicts in internet governance: Liberals vs. sovereigntists?, *Global Constitutionalism*, 9, 2 (2020).

[8] Article 19, Mexico: Army used Pegasus spyware against journalists and activists, 4 October 2022, https://www.article19.org/resources/mexico-army-spyware-journalists-activists.

[9] Jennifer Holleis, How cybercrime laws are silencing dissent in Mideast, DW, 13 May 2022, https://www.dw.com/en/how-cybercrime-laws-are-used-to-silence-dissent-in-middle-east/a-61761603.

[10] See https://globalinitiative.net/initiatives/un-cyberwatch/.

[11] Alina Clasen, UN Cybercrime Convention calls EU values into question, civil society warns, EURACTIV, 19 December 2023, https://www.euractiv.com/section/cybersecurity/news/un-cybercrime-convention-calls-eu-values-into-question-civil-society-warns/.

[12] See Russia's draft treaty: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Russian_Fed_statement_-3rd_session.1.pdf.

[13] See Statement by the Delegation of the Russian Federation at the end of the 6th session of the UN Ad Hoc Committee on the elaboration of a universal convention on combating information crime, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Statements/Russian_Federation_E.pdf.

[14] See Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Sixth Session, Statement delivered by Canada, 1 September 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Statements/Canada_E.pdf.

[15] Summer Walker, Still poles apart: UN Cybercrime Treaty negotiations, June 2023, https://globalinitiative.net/analysis/un-cybercrime-treaty-negotiations/.

[16] Such as on a review mechanism, under a working group in which H.E. Mr. Raphaël Nägeli, ambassador and permanent representative of Switzerland to the United Nations, Vienna, and Mr Terlumun George-Maria Tyendezwa, Deputy Director of Legal Service, Federal Ministry of Justice of Nigeria, and Vice-Chair of the Ad Hoc Committee, were the co-facilitators of the informal negotiation, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Informal_negotiations/Group_E/AHC_co-facilitated_negotiating_Group_E_report.pdf.

[17] See Sixth session of the Ad Hoc Committee: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main.

[18] Deborah Brown and Katitza Rodriguez, UN cybercrime treaty: A menace in the making, Euractiv, 16 October 2023, https://www.euractiv.com/section/cybersecurity/opinion/un-cybercrime-treaty-a-menace-in-the-making/; Tech Accord, Press release: Cybersecurity Tech Accord expresses continued concern over latest draft of UN Cybercrime Treaty, calls for extensive changes, 12 December 2023, https://cybertechaccord.org/cybersecurity-tech-accord-expresses-continued-concern-over-latest-draft-of-un-cybercrime-treaty-calls-for-extensive-changes/.

[19] UN General Assembly, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the

Use of Information and Communications Technologies for Criminal Purposes, Revised draft text of the convention, 6 November 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/084/92/PDF/V2308492.pdf?OpenElement.

[20] UN General Assembly, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft text of the convention, 29 May 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/039/51/PDF/V2303951.pdf?OpenElement.

[21] 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/.

[22] UN General Assembly, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Revised draft text of the convention, 6 November 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/084/92/PDF/V2308492.pdf?OpenElement.

[23] GI-TOC, UN Cybercrime Treaty: Summary of the GI-TOC's key positions, November 2023, https://globalinitiative.net/analysis/un-cybercrime-treaty-gitoc-positions-nov-23/.

[24] UN General Assembly, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Revised draft text of the convention, 6 November 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/084/92/PDF/V2308492.pdf?OpenElement.

[25] Ibid.

[26] Canadian proposal submitted to the AHC at its sixth session. And submitted in writing ahead of the 7th session, supported by Australia, Chile, the Dominican Republic, the European Union and its Member States, Iceland, Japan, Liechtenstein, New Zealand, Norway, the United Kingdom, the United States, and Switzerland. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Canada_proposal_3.3.pdf.

[27] UN General Assembly, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Revised draft text of the convention, 6 November 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/084/92/PDF/V2308492.pdf?OpenElement.

[28] Ibid.

[29] Summer Walker, Closing Pandora's box: UN Cybercrime Treaty negotiations, August 2023, https://globalinitiative.net/analysis/un-cybercrime-treaty-negotiations-august-2023/.

[30] See United Nations Convention against Transnational Organized Crime and the Protocols thereto, Article 2, https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

[31] United Nations General Assembly, A/RES/75/282, 26 May 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement.

[32] Summer Walker and Ian Tennant, Control, alt, or delete? The UN cybercrime debate enters a new phase, GI-TOC, December 2021, https://globalinitiative.net/analysis/un-cybercrime-debate/.

[33] This committee has not negotiated any explanatory notes and there are apparently no plans for a *travaux preparatoires*. According to the Vienna Convention on the Law of Treaties, these documents can be used to supplement the interpretation of a treaty when the meaning is ambiguous or obscure. See Vienna Convention on the Law of Treaties, https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXIII-1&chapter=23&Temp=mtdsg3&clang=_en. The UNTOC, on the other hand, took 11 sessions and agreed to more than 100 interpretive notes to clarify and guide its implementation.

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