POLICY BRIEF

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

DATA OVERLOAD

UN NEGOTIATIONS ON CRIMINAL USE OF ICT TAKE OFF

Summer Walker

AUGUST 2022

ACKNOWLEDGEMENTS

Special thanks to the research team on country positions: Ana Paula Oliveira, Maria Velandia and Darren Brookbanks. Thanks also to Ian Tennant for his thoughtful review and feedback, and to the Global Initiative Against Transnational Organized Crime (GI-TOC)'s Publications team.

We would like to thank the UK Home Office for their support in funding this policy brief. This publication does not necessarily represent the views or policies of the UK Home Office.

ABOUT THE AUTHOR

Summer Walker is the GI-TOC's Head of Multilateral Affairs, in New York. She leads projects and provides research and analysis on international policy, with issues ranging from drug policy to cybercrime. As the New York representative, she engages with the UN and government missions to bring the research and innovative approaches of the GI-TOC and its Network of Experts to multilateral policy debates. She has worked in international policy for many years both at the UN, and with international NGOs, development agencies and research institutes.

Cover: © *Daniel Slim/AFP via Getty Images*

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

CONTENTS

SUMMARY

In early 2022, governments at the United Nations began negotiations to draft a global instrument to address cybercrime – or to 'counter the use of information and communications technologies (ICTs) for criminal purposes' – to use the official title of the process. The process, initiated by Russia and rejected by Western states in 2019,[1] has since seen all regional blocs come on board to try to shape a potential instrument. The first meeting in February and March 2022 was overshadowed by Russia's invasion of Ukraine in February. It resulted in a roadmap for the process and a decision on the potential sections of a future document, but not an overwhelming sense of shared purpose among member states. The second meeting, held from 30 May to 10 June, turned to the actual substance of the treaty, where though geopolitical divisions – particularly between Western countries and Russia – remained high, states found more common ground than was expected.

This meeting, which pressed states to take positions on specific content for the first time, occurred following decades of inertia based on strong disagreements over the need for a UN treaty. Differences stem from a lack of common vision on the parameters of cybercrime, internet governance and digital sovereignty, as well as for regulation of online content and access to data. At their core, these concerns boil down to issues of state control – in terms of cooperation and data sharing with other states and in relation to countries' control over their own citizens' data.[2]

So it may be surprising that governments across regional blocs may be opening themselves up to an instrument with a broad scope and wide parameters for cooperation on crimes committed using information and communications technology (ICT). This apparent shift occurred after governments first outlined strong, and divergent, positions on which crimes should be listed under this treaty – with the predictable blocs on the furthest ends of the spectrum, the European Union (EU) proposing a narrow convention focused on cyber-dependent crimes, and Russia and allies proposing a wide scope of crimes covered, including content-related crimes, cyber-enabled crimes and national security threats such as terrorism. However, when moving onto procedural measures, many states shared the position that procedural measures and collection of electronic evidence should apply to all crimes or all serious crimes committed using ICT. Only the EU (including France and Czechia speaking independently) and Malaysia stood out as rejecting this idea.

This position tracks more fundamentally with the wide scope proposed by Russia. It includes opening the door to cooperation on many crimes – which a number of countries had previously said they did not want covered in the treaty. Adopting a narrowly defined set of crimes to be covered under the convention's criminalization provisions has been a central position for countries pursuing a treaty with human rights and fundamental freedoms at its core. This approach could well be at risk if the rest of the treaty incorporates a wide scope of crimes. Some questions that this raises are:

- If the sections following criminalization apply to a wider spectrum of crimes, what is it that a criminalization section will support or achieve?
- Can existing instruments be used to increase investigative and prosecutorial procedures, and international cooperation, for crimes committed using ICT. What, then, needs to be in a new instrument?
- How will duplication of UN agency responsibilities and siloed approaches be avoided when splitting cyber-enabled crimes between multiple regimes?
- Where would a line be drawn so this instrument does not become a tool used by some for cross-border cooperation on political repression and digital rights more broadly?

BACKGROUND

The vision outlined by the UN Ad Hoc Committee (AHC), which has been constituted to oversee the negotiations, is that the May 2022 meeting, together with another to be held in August to September 2022 will provide the basis upon which the AHC will develop a 'zero draft' to share with member states and stakeholders possibly by the beginning of 2023. The May meeting focused on a pre-agreed set of issues: criminalization; general provisions; and law enforcement and procedural measures. The August meeting will address the rest of the issues that the AHC had agreed should be covered by the treaty. These are international cooperation; technical assistance; preventive measures; the mechanism of implementation; and the final provisions and the preamble. These eight sections will form the basis for the instrument.

Broader relevance for international law

The process is important for two key reasons. At the UN, there is no universal instrument that has addressed the dramatic shifts in society, politics and the economy caused by information technology, and most specifically the internet. There have been significant efforts to create a body of standards and norms across contexts through working groups and resolutions: cybersecurity, cybercrime, bridging the digital divide, and digital rights and freedoms. But this treaty will be the first binding, global cyber-related instrument.

And that is relevant particularly because even though we increasingly live online, there is no international agreement affording positive rights in the cyber context, such as on digital freedoms and the right to privacy, from political campaigns to classrooms. There is also no right to access, and nearly a third of the global population have never used the internet as of 2021,[3] and two-thirds of school-age children in 2020 were without internet access at home.[4]

Outside the UN framework, there exists a global patchwork of digital regulations, which in many parts of the world can be highly invasive, such as surveillance capitalism[5] or state-controlled digital surveillance (here, the EU's General Data Protection Regulation is a welcome exception). A government's ability to shut down access to the internet or specific sites by controlling access points has increased with technology such as internet kill switches, which shut down access to

the internet, and internet shutdowns by governments have become increasingly common.[6] The global community is negotiating a framework to criminalize the use of ICT for criminal purposes. So while rights around the use of ICT have never been universally established, the debate on restricting actions – and possibly also rights – through a criminalization framework has begun.

The second reason this process is important is that cybercrimes are becoming more destabilizing, so confronting them requires a transnational approach with earnest cross-border cooperation. Ransomware attacks on hospital systems can impact hundreds or thousands of individuals as well as key social infrastructure. Financial fraud can wipe out people's savings. And often these crimes take place and are resolved out of the public eye. Regional and bilateral cooperation exists, most notably the Council of Europe's Budapest Convention, but a framework for global norms on cooperation does not. If this treaty, or protocol, can establish a minimum level of guidance and cooperation for states that find it most difficult to engage, and with greater transparency, it could prove a useful tool for wider society.

However, the challenges facing such cooperation are numerous. There is still no shared definition of cybercrime, nor is this process explicitly covering cybercrime, but rather countering the use of information and communications technologies (ICTs) for criminal purposes. This process, first initiated by Russia, with Western countries voting against it, formally began as the war in Ukraine had just begun. Negotiations are taking place at an extreme low point for multilateralism and at a time when there are increasing challenges for the protection of and espousing of positive rights in the digital space, coupled with a dramatic rise of digital surveillance activity by governments, data brokers and companies.

It is in this context that this treaty negotiation builds on decades of efforts at the UN and within regional bodies to try to create norms around cybersecurity and cybercrime in a way that bridges fundamental disagreements by laying down some general rules of the road that governments are expected to follow. This treaty, however, adds significant pressure to the debate because it would be a binding global instrument.

The May Ad Hoc Committee meeting

The May meeting of the AHC (30 May to 10 June) was the first to delve into the substance of the potential treaty, and was structured around three pre-selected topics: general provisions; criminalization; and law enforcement and procedural measures. The committee allocated the first day for opening statements, then moved on to state reactions to detailed lists of questions for each of the three topics. These questions were informed by previous submissions from and consultations with member states. The questionnaires were not always grouped in an obvious way, but the aim appeared to be to collect specific inputs from governments to shape a first draft of an instrument.

This brief provides an overview of that meeting, and addresses each of the three topics, highlighting key issues and outlining the general positions that were offered by states. It is not a comprehensive rendering of states' positions, but does attempt to show where areas of consensus are forming and where divergence is greatest on key topics.[7] Below, the brief starts with criminalization, then addresses law enforcement and procedural measures, followed by general provisions.

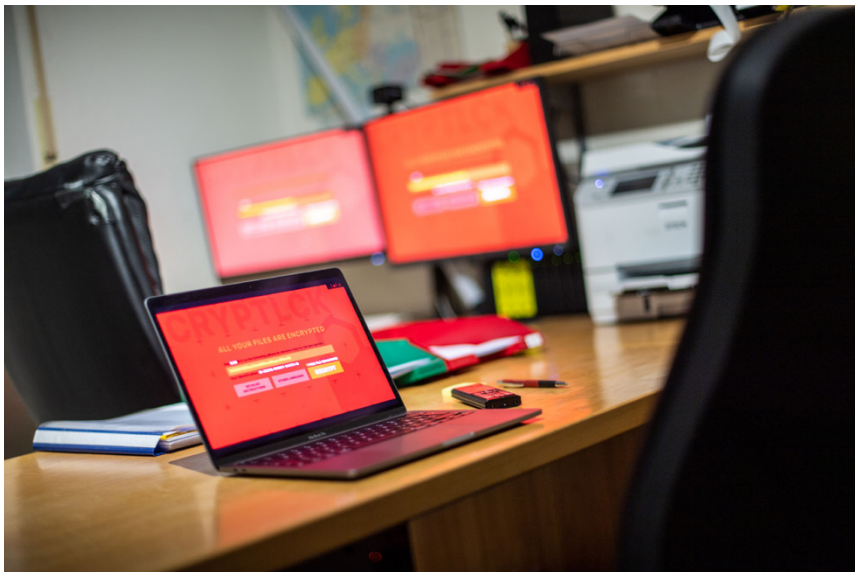
PROVISIONS ON CRIMINALIZATION

A section on criminalization is key to the treaty's role in establishing norms, since this is where governments would list the crimes covered under the convention. A consensual understanding of cyber-dependent or -enabled criminal activities could provide states with tools to prevent or prosecute crimes more effectively. However, criminalizing certain activities risks being abused by states to establish international norms that allow crackdowns on dissent, or the stifling of media, political debate or opposition movements by applying cybercrime laws. The criminal activities covered in this section are therefore critical. It is much more difficult to undo what has been written into a treaty than adapt and update it through resolutions.

After observing the May meeting of the AHC, it is not entirely clear, however, how the criminalization section will be applied. A section on criminalization could frame the limits around which the entire convention is bound – that international cooperation, technical assistance and all articles in the treaty are limited to cooperation on these crimes. At the national level, it can require signatories to take measures such as drafting legislation criminalizing the listed activities and developing sanctions around them (e.g. fines, prison sentences). Or, for international cooperation, it could set out the crimes for which governments will enhance cooperation with other governments and direct technical assistance to other countries (not least by UN agencies). For a crime treaty, this would typically frame the rest of the treaty, but this does not appear to be the case, since, when governments switched to discussions on procedural measures, many expressed a general willingness to cooperate on an indeterminate list of crimes committed using ICT. So while it is difficult to answer now how the section will apply to future treaty implementation, the current positions of states on criminalization show a spectrum of opinions on what they want included.

Positions along a spectrum

Many states exhibited strongly held positions on which crimes should be part of this convention, while some expressed an openness to hear others' positions as the negotiations continue. On one end of the spectrum is Russia and its allies, which support the inclusion of a wide range of crimes. Russia submitted a draft text in July 2021, which has now become the joint submission of Russia, China, Belarus, Burundi, Nicaragua and Tajikistan. This draft includes a vast range of crimes: cyber-dependent crimes and cyber-enabled crimes, such as drug trafficking online or arms



Ransomware attacks have crippled entire institutions.
© credit Lino Mirgeler/Picture Alliance via Getty Images

trafficking online; child sexual exploitation online; incitement to suicide; incitement to subversive activity; terrorism-related offences; extremism-related offences (which includes distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic or religious hatred or enmity); and rehabilitation of Nazism (Russia's apparent 'justification' for war in Ukraine).[8] In negotiations, Venezuela, Burkina Faso, and Eritrea expressed support for this wide list of crimes.

There are other countries that also do not want a limited scope of crimes, but simultaneously are not comprehensively aligned with the Russia draft. India also supports inclusion of a wide-ranging list of crimes, and submitted a draft that includes crimes such as 'sending offensive messages through communication service' and 'publishing or transmitting material containing sexually explicit acts, etc, in electronic form' supports including a wide range of crimes, with a particular focus on terrorism-related offences.[9]

Meanwhile, there is another group of countries that want national security issues to be included in the treaty, such as terrorism-related offences, but they do not vote as a bloc. This grouping includes Peru, Panama, India, Israel, Indonesia, Sudan and Jordan, for instance. Kenya stated it wants both cyber espionage and cyber terrorism included. Some states that called for terrorism-related offences also want to include incitement to terrorism (a content offence), such as Israel and El Salvador.

Categories of cybercrimes

- *Cyber-dependent* crimes threaten the confidentiality, integrity and availability of data and systems.
- *Cyber-enabled* crimes encompass offences that also occur offline, but in which criminals may deploy technology to achieve their ends.

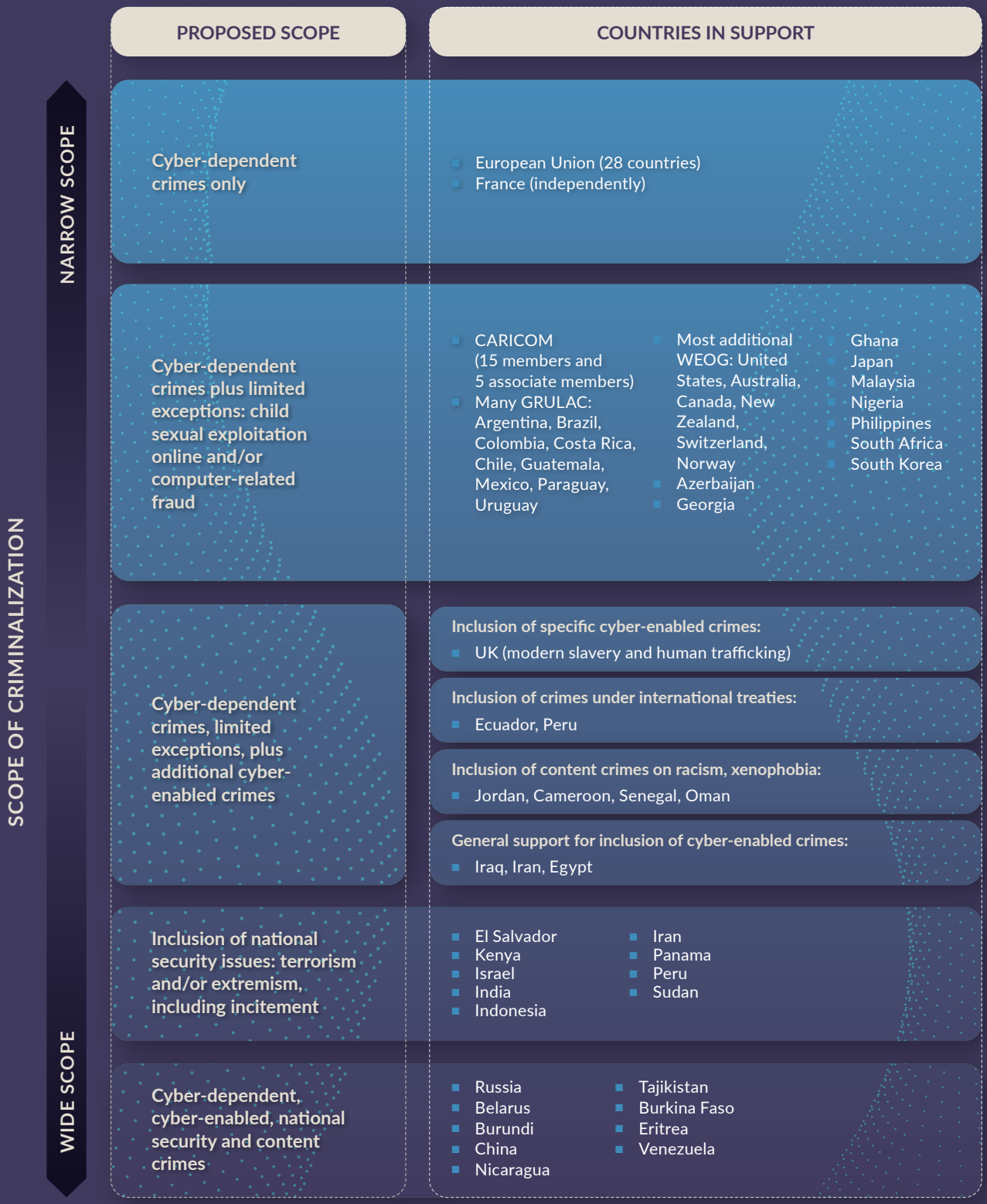


FIGURE 1 Which cybercrimes should be part of a convention?

NOTE: This list is not exhaustive.

Another grouping of governments, although not necessarily aligned with one another, are open to the inclusion of more cyber-enabled crimes, but not the same crimes. For instance, the UK included a 'comment' (rather than a proposed article) in its submission, saying it would like to see provisions to criminalize modern slavery and human trafficking, and to address unauthorized sharing of intimate images.[10] A handful of other countries, one being Ecuador, expressed an interest in including cyber-enabled crimes covered in other conventions. Others expressed a willingness to hear the perspective of states that want this, such as Australia, Brazil, or Azerbaijan, which rejected an expansion in principle but were open to it if consensus were reached.

On the other end of the spectrum is the EU submission, which calls explicitly for inclusion of cyber-dependent crimes only, a position that is also vocally supported by France. These crimes require use of a computer system to commit them, encompassing crimes such as illegal access and illegal interference. Closely alongside this position are a number of countries, including Japan, South Korea, the Philippines, most Western countries (members of WEOG), and many Latin America and Caribbean ones (GRULAC),[11] including the Caribbean Community's (CARICOM) joint position. These states support cyber-dependent crimes plus the cyber-enabled crimes of child sexual exploitation online and/or fraud committed online (such as financial fraud). Leaning in this direction but open to discussion on topics such as incitement or racism are countries such as South Africa and Nigeria, key players in the African Group bloc.

A comment on child sexual exploitation online

Despite objecting to the inclusion of cyber-enabled crimes more generally, Australia, Canada and the United Kingdom took the lead in supporting the inclusion of child sexual exploitation online. As long as it remains narrowly defined, there seems to be significant consensus across regional blocs for its inclusion. Child sexual abuse material (CSAM) is listed in the Budapest Convention. France, however, along with several digital rights organizations, has taken a harder line on including any cyber-enabled crime, including CSAM, because this would open the door to the inclusion of other cyber-enabled crimes. France argued that the Convention on the Rights of the Child optional protocol already addresses this form of criminality. Some countries want the inclusion of a further set of crimes in this context, with Brazil and Uruguay calling for inclusion of incitement to suicide, and Mexico calling for sexual extortion in this context.

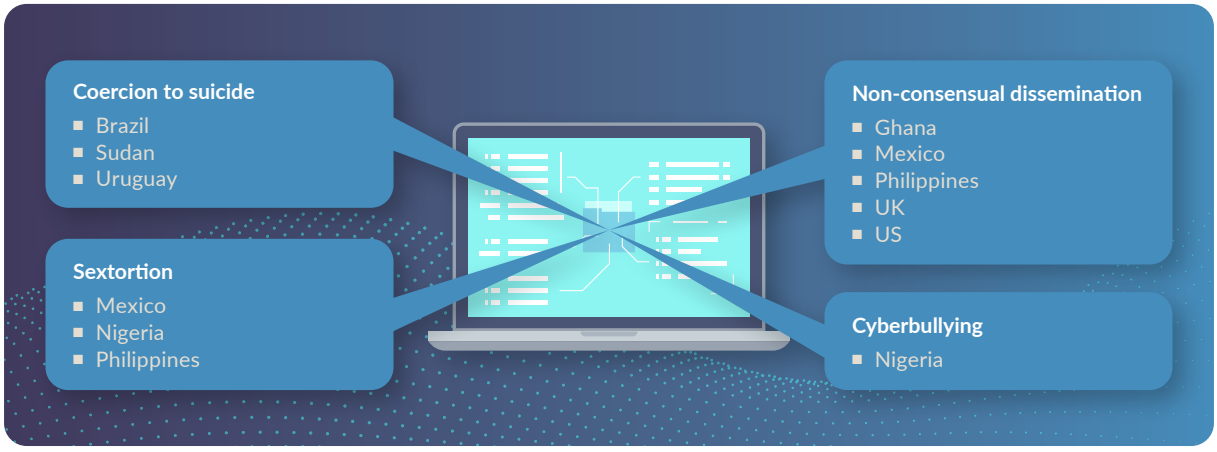


FIGURE 2 Additional crimes proposed to be included under child sexual exploitation.
NOTE: This list is not exhaustive.

PROVISIONS ON LAW ENFORCEMENT AND PROCEDURAL MEASURES

Most states supported broad cooperation on law enforcement, procedural measures and electronic evidence, which was a significant departure from the previous week's discussions on criminalization. The chair posed a question on whether the scope of the chapter on procedural measures and law enforcement should apply to offences beyond those listed in the instrument. Perhaps surprisingly, many states across regional blocs believe the scope should apply beyond the offences covered in the convention. Or perhaps not, since the Budapest Convention allows for broader procedural cooperation beyond the crimes enumerated in the treaty.[12] But that convention was drafted largely in the spirit of cooperation, something that eluded the origins of this process – and these types of choices will impact the reach of a new global instrument beyond procedural measures.

Many states pointed to the UNTOC and UNCAC for this section, signalling that language can be borrowed to develop a first draft. For instance, CARICOM countries, Australia and India, among others, all agreed that jurisdiction articles from UNTOC and UNCAC could form a basis for discussion. States pointed to articles on witnesses and victims from these conventions as well. In other areas, such as asset freezing and confiscation, there was a range of views and a general feeling that these specifics will be taken up later in the process.

Electronic evidence

During discussion on procedural measures, as well as during the general provisions debate, it became clear that the holy grail of this process for many countries is gaining cross-border access to electronic evidence. In fact, a second optional protocol to the Budapest Convention on this has just been opened for ratification in May 2022 (after four years of negotiation) in response to calls for enhancing (i.e. speeding up) cooperation for collecting evidence. Some countries, such as India and Angola, made clear that their main interest of a convention is electronic evidence sharing.

Electronic evidence sharing raises issues of jurisdiction, transborder access to data, sovereignty and the ability to compel private companies to cooperate. Service providers, data and involved parties often sit in different jurisdictions, and therefore have different regulations for privacy

protection and regulations on what constitutes warranted access to data. From a rights-perspective, there is a concern that procedures, including evidence sharing, in a new instrument will not have sufficient safeguards for privacy protection, prioritizing law enforcement expediency above citizen rights. As said in the submission by Electronic Frontier Foundation, 'human rights should not be harmonized to the lowest common denominator in cross border investigations'.[13]

On the other hand, states that are focused on sovereignty rights view accessing their citizens' data (stored by a foreign multinational, for example) without governmental consent as a breach of national sovereignty (many of these states have made efforts to bring servers for private companies into their national territory).[14] Yet all these states want the ability to access data and evidence when they need to. The traditional process of sharing evidence is through a mutual legal assistance treaty, which many states claim is too slow for electronic evidence, but has been the standard bearer for judicial safeguards and investigative cooperation.

Within this context, there was wide support that electronic evidence should cover most or all crimes committed using computer systems – which would include cyber-enabled crimes and possibly content crimes, which many are adamant should not be criminalized in the treaty. For instance, some states who support a treaty focused primarily on cyber-dependent crimes supported this compromise, including CARICOM, United States, Chile and the Philippines. As stated above, this view is a departure from attempts to narrowly define the crimes covered in a future treaty. There were some hold-outs: France, the EU and Malaysia stated that electronic evidence should be limited to the crimes in the treaty, while Czechia also agreed but said it remained open to others' views.

While in many cases, the Committee collected fairly detailed positions from states, ranging from how they would define intent or include intent (mens rea, to use the legal term) in the criminalization section, or if asset forfeiture should be a procedure in the treaty, there is still an overarching, unanswered question of what this treaty is supposed to do. This stems from the dichotomy of willingness for cooperation across crimes while at the same time a significant amount of states are arguing for a narrow treaty.

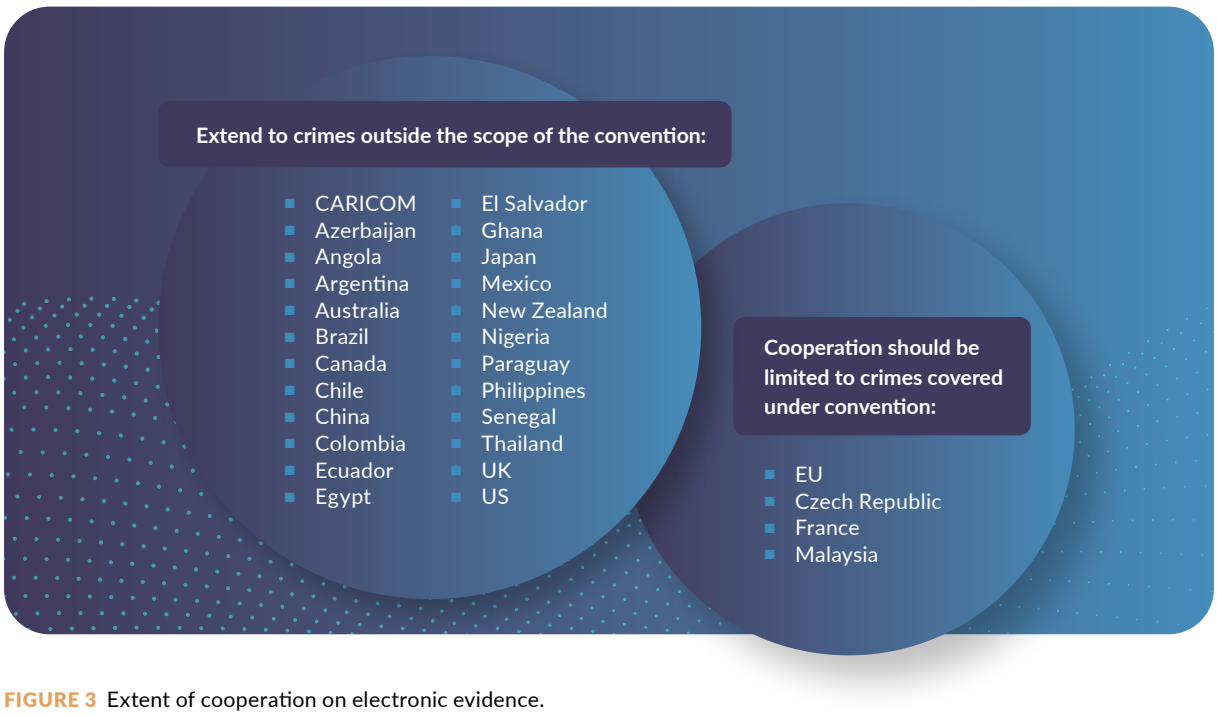


FIGURE 3 Extent of cooperation on electronic evidence.
NOTE: This list is not exhaustive.

Human rights, legal safeguards and judicial oversight

The chair posed a question on whether provisions in this section (law enforcement and procedural measures) should be subject to specific legal principles, such as proportionality or references to human rights obligations. A similar grouping to the countries that support a narrow convention agreed there is opportunity for both types of articles, including the EU, Japan, Argentina, Costa Rica and Colombia. There is also a group of countries, such as Paraguay and Mexico, that supported specific legal principles such as necessity and proportionality, but did not support references to human rights treaty obligations. Going further, Canada noted that privacy protections should be precise, and the US was open to hearing perspectives on how to protect privacy while at the same time protecting society from crime. When discussing procedural measures, South Africa, Nigeria and the EU raised the importance of judicial oversight, a critical area for the protection of civil and political rights. Some countries expressed that safeguards should be in line with previous conventions, but there is a question of which conventions they have in mind – the Universal Declaration of Human Rights or UNTOC – and whether specific safeguards are necessary in the digital space.

People take to the streets in India to protest against the government's alleged use of spyware against certain groups, July 2021. *© Sumit Sanyal/SOPA Images/LightRocket via Getty Images*

Examples of potential safeguards

- Dual criminality: Requesting and receiving countries share criminal offences in their codes[15]
- Necessary and proportionate actions: That a balance is struck that chooses the least restrictive measure; and is necessary to carry out an investigation
- Judicial oversight and due process
- Transparency and oversight by a third party (with decision-making ability)
- Privacy protections (something many states themselves do not strongly regulate)

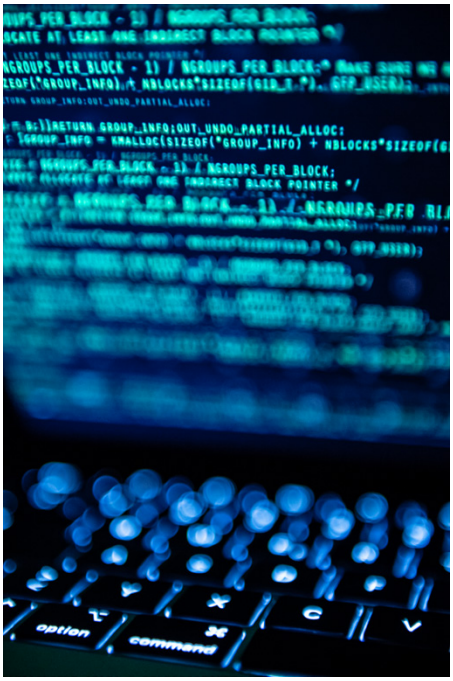
GENERAL PROVISIONS

States' positions on general provisions were largely aligned, but the devil is in the detail. General provisions in UN crime-focused treaties typically address the overall purpose, definitions of terms, the scope of application and sovereignty. This was the area where governments shared most common ground in their positions, and were generally supportive of relying on agreed-upon language from UNTOC and UNCAC, including on the issue of sovereignty. There was a consensus forming around an overall purpose, but the thorny issue of establishing definitions of terms was deferred to a later stage in negotiations.

Purpose of instrument

Member states appeared to be in relative agreement on the overall purpose of the treaty, which would have three main objectives: combating and preventing crimes committed using ICT (or cybercrime); promoting international cooperation; and technical assistance. Some countries supported including specific issues such as cross-border data in the purpose of the treaty, such as Paraguay; whereas a number of others signalled that cross-border evidence should be addressed in the scope of application.

Pakistan stated an interest to include prevention in the purpose, while the EU proposes a clause on supporting victims' rights in the purpose. Yet, overall, the three main objectives appeared to have a strong level of consensus among governments. Many states, such as Australia, Thailand and the United Kingdom, echoed a sentiment that the purpose and scope sit firmly within criminal justice and should not stray into internet governance or cybersecurity. Within this relative agreement, there were countries that advocated for using the term 'cybercrime' to align with existing treaties (Budapest Convention) and the work of the UN's Open-ended Intergovernmental Expert Group Meeting on Cybercrime in Vienna. This faced strong pushback from Russia, which believes the title of the AHC process should lock in the language for the treaty.



A hacker program seen on a computer screen. *© Silas Stein/Picture Alliance via Getty Images*

Definition of terms

Where governments were – and are – bound to have significant disagreement is in the definition of terms used in the proposed treaty. These questions relate to the issues of how broad the convention will be, what norms it will set for cyber issues and how much will be taken from existing agreements or redefined. Here the West vs Russia polarity emerged again, with questions on terminology often posed to ask states if they prefer language set in the Budapest Convention or language set in the Russia draft convention. One example of this was whether a convention should use the term 'computer data' (which is used in the Budapest Convention)[16] or 'digital information', which is Russia's preferred expression. The chair also posed a question to states on a procedural level, which found relative consensus – which was whether definitions should be addressed at a later stage after substantive articles are negotiated. Therefore, positions on definitions will re-emerge later in the process.

Sovereignty

Protection of sovereignty is an article included in the general purposes of UNTOC and UNCAC. China in particular is a champion of non-intervention and sovereignty clauses in agreements and in policy debates. On the issue of sovereignty in this context, most countries were satisfied with using the language from UNTOC and UNCAC as the basis, including China, Japan and the United States. However, sovereignty rights are rather more complex in the context of cybercrime (or countering crimes using ICT), because the data of one country's citizens may sit in another jurisdiction with a multinational tech company or be held in the cloud, for instance. Some countries, such as Angola and New Zealand, noted the unique nature of cyberspace, such as transnational infrastructure and its virtual cross-border nature, as a reason to consider new language. It appears the language from UNTOC or UNCAC will serve as the basis.

UNTOC Article 4: Protection of sovereignty

1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.
2. Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.[17]

Human rights provisions

On human rights provisions, countries across regional blocs supported references to human rights in the general principles, and were open on how and where to include these references. For instance, the United States requested an article in the general principles committing to implement the entire treaty in line with human rights obligations and recommended an overarching commitment, including to the International Covenant on Civil and Political Rights. Japan called for the inclusion of due process and human rights in the guiding principles. Meanwhile, many other governments called for alignment with UNTOC and UNCAC on protections for journalists and whistle-blowers. Some were more cautious, calling for a balance between law enforcement and human rights (Ghana and Malaysia being examples). Some countries, including China, that said that human rights provisions do not fit in general provisions, and that they should be addressed in other sections. There seemed to be a general understanding that human rights protections will be in the instrument – the question is where and how robust these measures will be. Some of this will be reflected in how strong the safeguards are in the instrument, rather than an overarching reference in general provisions or a future preamble. Hence it is important to observe the safeguards discussions in the previously held procedural mechanisms debate and the upcoming international cooperation debate.

Some parties are in favour of a treaty that would protect people's privacy while simultaneously shielding society from cybercrime.
© Andriy Onufriyenko via Getty Images

After this first meeting, it appears the committee has a general consensus forming around the format for the general provisions, but as became clear in the detail, terminology and definitions will throw up obstacles in the future negotiations.

CONCLUSION

At the end of August 2022, states and stakeholders will reconvene to discuss

- international cooperation;
- technical assistance;
- preventive measures;
- the mechanism of implementation; and
- the final provisions and the preamble.

This meeting will continue to shed light on what the purpose of this instrument will be. Considering the ongoing disagreements regarding criminalization (i.e. which types of crime to define and specifically make illegal under the treaty), the willingness of many governments to include a broad scope of crimes in other provisions – on cooperation and electronic evidence, for example – points towards a potentially wide-ranging instrument.

Promoting a narrowly defined set of crimes covered under the convention's criminalization provisions has been a central position of those countries pursuing a treaty with human rights and fundamental freedoms at its core. This could be at risk if the rest of the treaty has a wide scope of crimes, and should be considered carefully.

While governments coalesced around an overall purpose largely in sync with earlier crime treaties like UNTOC, fundamental and important questions remain on what is being cooked in the kitchen: will this be a technology-focused supplement to existing treaties in the crime space? Is it a new treaty to address crimes that are not covered under existing agreements? And if it is both – how would that work? Some questions this raises are:

- If the sections following criminalization are focused on a wider spectrum of crimes, what would the criminalization section of the treaty support or do?
- Can existing instruments be used to increase investigatory and prosecutorial procedures, and international cooperation, for crimes committed using ICT. What, then, needs to be in a new instrument?
- How will states avoid duplication of UN agency responsibilities and siloed approaches if splitting cyber-enabled crimes between multiple regimes?
- Where would a line be drawn so this instrument does not in fact become a tool used by some for cross-border cooperation on political repression and digital rights more broadly. How will limits be set to its reach?

NOTES

1 United Nations General Assembly, 52nd plenary meeting, 19 December 2019, A/74/PV.52, p 37.

2 For more background see, Summer Walker and Ian Tennant, Control, alt, or delete? The UN cybercrime debate enters a new phase, GI-TOC, December 2021; Summer Walker, Cyber-insecurities? A guide to the UN cybercrime debate, GI-TOC, March 2019.

3 Nearly 1 in 3 people have never used the internet, UN agency estimates, *The Washington Post*, 1 December 2021, livehttps://www.washingtonpost.com/world/2021/12/01/global-internet-usage/.

4 UNICEF, Two thirds of the world's school-age children have no internet access at home, new UNICEF-ITU report says, 30 November 2020, https://www.unicef.org/press-releases/two-thirds-worlds-school-age-children-have-no-internet-access-home-new-unicef-itu.

5 For instance, see Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Hachette Book Group, 2019.

6 Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights, 23 June 2022, OHCHR, https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human.

7 The references to states positions derive from attendance at the AHC, 30 May to 10 June. The webcast for the event and country positions submitted prior to the meeting can be found at the link below. We have added references for content from written submissions, but refer to this footnote for remarks made at the meeting. See Second session of the Ad Hoc Committee, Vienna, 30 May to 10 June 2022, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

8 For a copy of this draft, see https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf.

9 Indian contribution for 2nd Session of AHC, Criminalization, General Provisions and Procedural Measures and Law Enforcement, UN Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Indian_Draft_Text_for_UN_AHC_for_2nd_Session.pdf.

10 See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/United_Kingdom_contribution_E.pdf.

11 UN regional groups: WEOG: Western European and Other Group; GRULAC: Group of Latin America and the Caribbean.

12 See, for instance, Article 14 Scope of procedural provisions, Budapest Convention, https://rm.coe.int/1680081561: 'Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: (a) the criminal offences established in accordance with Articles 2 through 11 of this Convention; (b) other criminal offences committed by means of a computer system; and (c) the collection of evidence in electronic form of a criminal offence.'

13 Katitza Rodriguez and Tomaso Falchetta, Submission by Electronic Frontier Foundation and Privacy International to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose; see https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/EFF_contribution.pdf.

14 Summer Walker, Cyber-Insecurities? A guide to the UN cybercrime debate, GI-TOC, March 2019.

15 This safeguard does not protect citizens' rights if two countries share laws making political dissent illegal in cybercrime laws, for instance. If there was a UN or international clearing house for exchanging data for evidence, how would this be addressed?

16 For a copy of the convention, see https://rm.coe.int/1680081561.

17 For a copy of the convention, see https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 500 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