



**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

UN 'CYBERCRIME TREATY'

LEGAL AND HUMAN
RIGHTS SAFEGUARDS

ROUNDTABLE, 30 MARCH 2023

Meeting report drafted by
Ana Paula Oliveira and Summer Walker

MAY 2023

ACKNOWLEDGEMENTS

The Global Initiative Against Transnational Organized Crime (GI-TOC) would like to thank the participants for joining the roundtable and sharing their expert views on the issues. This roundtable was supported by the United Kingdom Home Office. The views expressed do not necessarily reflect the views of the United Kingdom Home Office.

ABOUT THE AUTHORS

Summer Walker is the GI-TOC's Head of Multilateral Affairs in New York. She leads projects and provides research and analysis on international policy, with issues ranging from drug policy to cybercrime. She has worked at the UN and with international NGOs, development agencies and research institutes.

Ana Paula Oliveira is an analyst at the GI-TOC. She conducts research with a focus on assassinations, disappearances and other forms of violence in the context of illicit economies. Her research interests also involve the impact of organized crime on human rights, and humanitarian law and policy. Before this, she practised at a law firm focusing on public law litigation. Ana Paula has an LL.M *cum laude* in international law from the Graduate Institute of International and Development Studies in Geneva, an LL.M in public law and an MBA in international relations from Fundação Getúlio Vargas in Rio de Janeiro.

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

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

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

CONTENTS

INTRODUCTION POINTS	4
KEY OVERALL POINTS	5
Scope for cooperation	5
Inconsistency in terminology	5
References to human rights law.....	5
INTERNATIONAL COOPERATION AND MUTUAL LEGAL ASSISTANCE	6
Procedural measures	6
Data protection	7
TECHNICAL ASSISTANCE	8
MECHANISM FOR IMPLEMENTATION.....	8
OVERARCHING CONCLUSIONS	9



INTRODUCTION

In March 2023, the GI-TOC held a roundtable to consult experts in human rights, digital rights and criminal justice on the legal and human rights safeguards in the consolidated negotiation document proposed by the Ad Hoc Committee (AHC) for a treaty to counter the use of Information and communications technologies for criminal purposes (broadly referred to as the ‘cybercrime treaty’). This expert consultation enabled a review of the current draft document and the negotiation process from the perspectives of digital rights, international and criminal law, and the private sector. It also allows us to see where consensus among multistakeholders is forming on the issue of human rights and legal safeguards in the process of negotiating the cybercrime treaty.

In January 2023, governments convened to outline their positions on the first part of the consolidated negotiation document. There was resistance from some states and groups of states to include human rights or legal safeguards (or the value thereof); others countered such resistance vocally. The resistance to these safeguards poses several risks. The first is that no international crime treaty should be without built-in legal safeguards. Secondly, the draft, as it stands, contains very permissive language for governments to cooperate in legal cases, technical assistance and general cooperation, potentially allowing for it to be used to suppress freedom of expression, association and political dissent. And, thirdly, this will be the first binding international treaty that governs cyberspace in any form. Any dialling back of safeguards during this early stage of the process, coupled with a draft that promotes expansive cooperation, risks creating a weak instrument in terms of human rights protection measures – and one that may be ratified by enough states to be codified in international law.

The focus of discussions was the second part of the draft text (yet to be negotiated at the time of the consultation), while including thoughts on the already debated text. The objective of this roundtable was to contribute ideas on safeguards to the negotiating process as negotiations proceed in the AHC.

The sections that follow provide a summary of the findings from the meeting.



KEY OVERALL POINTS

Scope for cooperation

A main concern expressed by participants was the broad scope of the proposed instrument set out in the draft text. As it stands, the document does not confine the scope to cyber-dependent crimes, which has been a call from civil society private-sector actors, but includes offences such as civil and administrative offences that are not criminal in nature. It also includes the provision to gather electronic evidence for crimes outside the proposed convention, but without providing clear guidelines on which crimes. This broad scope could lead to human rights repercussions. Firstly, it makes requirements such as dual criminality difficult to be implemented in practice and time-consuming for government officials. The latter is compounded if articles on spontaneous information, emergency mutual legal assistance and other rapid response clauses remain, meaning requested governments will be pressured to act quickly. Secondly, it allows for the possibility of cooperation for a wide range of activities, beyond those that are categorically criminal, including political, social and cultural actions that some governments may deem as criminal. This might breach guarantees around data protection and lawful use of personal information, and infringe human rights principles and guarantees.

Inconsistency in terminology

A second overarching point expressed by participants was the inconsistency in terminology used to refer to those in possession of data. Private-sector representatives expressed their concern with the use of terms used such as 'service providers' instead of 'data subjects' or 'data custodians'. Although there is a preference for using terminology such as 'data subjects', participants were mindful that there should be a clear distinction made between 'data subjects' and other terms to be decided on in the negotiation, such as 'accused person', 'person of interest', 'witness' or 'victims'. This is key to upholding the legal and human rights protections that are applicable to people in the different stages of a criminal procedure.

References to human rights law

It was recognized that some important guarantees are already included in the draft. One example is the requirement to destroy requested data after its use. However, the consensus was that there is a need to include more references to international human rights law and the principles of legality, proportionality and necessity across the board, and less to domestic law. Some participants noted that emphasising domestic law could be viewed as protective for governments seeking to limit cooperation, but it can also be used by governments to override otherwise binding safeguards that can be laid out in the treaty. One suggestion was to reduce references to domestic law, while another was to include obligations under international law in those parts of the text where domestic law is referenced.



INTERNATIONAL COOPERATION AND MUTUAL LEGAL ASSISTANCE

Given the timing of the roundtable consultation – held ahead of the AHC’s April 2023 meeting – there was a strong focus on the second part of the consolidated negotiating draft, and in particular the question of international cooperation.

Specifically related to the chapter covering international cooperation and based on the consolidated negotiation document, participants said they were not convinced that the convention would protect citizens from potential abuse of executive authorities. Participants were sceptical about inclusion of certain articles. It was observed that Article 78 (on special investigative techniques) was problematic, in that it could be potentially misused to legitimize mass surveillance through digital means, limit freedom of expression and allow for content removal (under paragraph 4). Article 74 (Mutual legal assistance in the interception of *[content data] [information in electronic/digital form]*) was seen as problematic, as it does not specify what kind of data is considered under this article. According to many participants, these articles should be deleted or substantially redrafted.

Procedural measures

A major concern voiced by participants was the lack of a streamlined human rights approach in the section on refusal to cooperate (Article 58, paragraph 15). Participants suggested that the treaty should set out mandatory conditions for refusal, including scenarios where there is a high likelihood of human rights violations occurring. One comparative source that could be drawn from is the UNODC’s model law on extradition, which builds on various extradition instruments and human rights jurisprudence on extradition.

Measures taken to access to information should take into account rights to freedom of expression and privacy. A possibility voiced was to make grounds for refusal applicable throughout the international cooperation section instead of incorporating them in some article and then risking missing it in relevant provisions.

It was noted the provisions on extradition included the potential option for states to refuse to extradite to protect their national interest, and that such provisions may – hypothetically – be used as a loophole to protect criminal proxies that assist state parties, including protecting cyber activity conducted on behalf of the state.

On mutual legal assistance, it was suggested the addition of a section to articles 61 (General principles and procedures relating to mutual legal assistance), 68 (Mutual legal assistance in the expedited preservation of stored *[computer data] [electronic/digital information]*) and 69 (Mutual legal assistance in the expedited disclosure of preserved traffic *[data] [information]*). This section would spell out how mutual legal assistance may be refused if the requested state party concludes that the execution of the request is likely to violate fundamental human rights of the data subject.

Regarding dual criminality, given that the scope is unclear and to protect due process, it was deemed important to establish that dual criminality is considered a necessary requirement and should be met in cases where states seek assistance.



One participant emphasized the need to adhere to the principle of transparency. This means if a request for personal data does not endanger the ongoing investigation or prosecution, the data custodian has the right to notify end users that their data is being requested by a government.

Data protection

Participants raised concerns over Article 57 (Protection of personal data). Although experts agreed that is extremely important for data protection to be included in the treaty, they recognized the drafting is a selective reading of what already exists in regional and national laws. They found it fails to take into account the complexity of data protection laws, and could undermine existing standards for data protection. Several therefore argued that including a set of prescribed articles on data protection could limit the international legal understanding of data protection, which would be counterproductive.

One well-received recommendation was to rather include general principles on data protection in the treaty. One suggestion was to reference agreed-upon data protection principles, such as transparency, legitimate purposes, and consent, and list existing documents, such as the Council of Europe's Convention 108 and the European Union's General Data Protection Regulation (GDPR). Another recommendation was that data transfer should be conducted without prejudice to existing data protection frameworks regulating cross-border data transfer, so that there is an integration and an acknowledgement of existing data protection frameworks.

It was suggested that the language around human rights in section 3 of Article 57 should be clarified in order to avoid potential misuse or public dissemination of personal data. The provision should make it clearer that the data obtained by a state cannot be used for any purposes other than those specified in paragraph 1 of the same article. This was deemed necessary to avoid an extensive interpretation that would allow for the use of data dissemination to prosecute political or state opponents, for example.



TECHNICAL ASSISTANCE

On technical assistance, participants were of the view that the provisions should expressly recognize the added value of civil society, including the private sector and academia. The argument is that civil society can impart knowledge and expertise in capacity building and technical assistance work. This recognition can be included in several provisions of the chapter. A recommendation made by some participants was to use the agreed consensus language on human rights and gender mainstreaming in other UN documents and approved by member states.

A specific concern from the private sector was regarding language in Article 85 (Expenses), which could allow mandatory or forced technology transfers, which could challenge private property rights. Article 86 (General principles of technical assistance) was also mentioned as containing language that can be interpreted as mandatory, and suggestions were made that these articles should align with the principle of voluntary capacity-building cooperation.

MECHANISM FOR IMPLEMENTATION


With regard to the mechanism for implementation, where the draft includes three options, some participants voiced concern over the option that proposes bringing the conference under the UN Commission on Crime Prevention and Criminal Justice (CCPCJ). Their concern rests on the fact that under current CCPCJ rules, this would limit the broader participation of civil society, including the private sector and academia. Participants agreed there is a need to include a *chapeau* in the draft that would summarise a mechanism of implementation that lays out involvement of multistakeholders.

Option 2 proposes a conference of parties with an 'International Technical Commission', with one-third representing members of the International Telecommunications Union (ITU), the UN's specialized agency for ICT. Participants who work across the UN's cyber-bodies voiced concern over including the ITU in an expert group. The ITU is a technical body and linking it so closely to a criminal justice treaty could lead to the politicization of its work. In the past, states have used the ITU to try to advance encryption-breaking and other politically motivated objectives. The feeling was that it is best to keep the ITU as a UN agency in implementation, but not to link it directly to the treaty.

Finally, participants discussed the need to include modalities for the review mechanism in the current draft rather than wait until it has been concluded and implementation begins. A review mechanism is a process where governments report on their progress in treaty implementation. Participants were of a view that at least a framework for review should be included in the text in order to avoid delays, as the experience with the UNTOC review mechanism only too evidently demonstrates. This framework must include multistakeholder participation.



OVERARCHING CONCLUSIONS

 One of the challenges faced by those in favour of a rights-affirming convention is that ‘each article is a moving target’. This means that provisions are linked to one another, and without knowing the outcome, it is difficult to predict which safeguards should be included and in which provision. However, the meeting enabled the following overarching recommendations to be identified:

- **A robust human rights framework is needed to counterbalance the broad powers conferred by the treaty.** There is a need for more references to human rights law and principles across the provisions, particularly in the international cooperation chapter. This treaty will establish norms and language upon which future cyber-based treaties be based, as is being done with the UNTOC and UNCAC in this drafting process. The consolidated negotiation document, as it stands, contains permissive language for governments to cooperate in legal cases, technical assistance and general cooperation, which risks criminalizing freedom of expression and association as well as political dissent.
- **There is a need to rethink the approach of selective reading.** Participants were mindful of the problem with replicating selective language from other instruments. The provisions of UNCAC and UNTOC were conceptualised to deal with a different range and scope of criminal activity. While language from these treaties is helpful as a starting point, this is a unique treaty and should be drafted as such.
- **Harmonize data access in line with human rights.** This convention can have added value if it streamlines and harmonizes rules on data access in this space in line with human rights safeguards.