



**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

2ND GUIDANCE NOTE ON A DRAFT CONVENTION ON CYBERCRIME

COVERING: INTERNATIONAL COOPERATION, TECHNICAL ASSISTANCE, PREVENTIVE MEASURES, MECHANISM OF IMPLEMENTATION, FINAL PROVISIONS AND PREAMBLE

A GI-TOC Contribution to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

JULY 2022

INTRODUCTION

The Ad Hoc Committee (AHC) has held two substantive meetings. By 1 July 2022, countries must submit their substantive contributions and proposed text on the second set of issues: International Cooperation, Technical Assistance, Preventive Measures, Mechanism of Implementation, Final Provisions and Preamble. This will be reviewed by the AHC chair and form the basis for the discussions on these issues at the next meeting of the AHC in New York, beginning on 29 August.

In this document, we consider this second set of issues, and offer ideas for consideration when drafting language for this treaty.¹

1. INTERNATIONAL COOPERATION

Facilitating international cooperation between diverse jurisdictions will be a key objective of this new legal instrument. The human rights and fundamental freedoms safeguards in the criminalization provisions will have to equally be applied in the section on international cooperation, where the framework for mutual legal assistance and extradition are expected to be laid out.

We offer the following contributions on international cooperation:

1. International cooperation provisions should have separate provisions related to cooperation for crimes covered and defined by the future convention, and for electronic evidence for a criminal offence, with stronger opt-out clauses for the latter based on domestic legal frameworks. For instance, extradition should not have flexibility.² States have shown willing to cooperate broadly on electronic evidence for crimes potentially not covered in this convention. Therefore, electronic evidence sharing should be clearly set out in its own provision, and not as an ‘and’ clause across the cooperation provisions, such as mutual legal assistance.

2. The provisions on international cooperation should aim to build trust by providing a framework for more transparent and multi-sectoral cooperation. Trust needs to be enhanced between governments and law enforcement agencies, and between law enforcement and the private sector, and can be built through an international cooperation framework that is more transparent and gives clear parameters for the exchange of information and evidence between different parties.³

3. Ensure safeguards on data protection, human rights and fundamental freedoms. The exchange of data entails a human rights and privacy risk, and requires robust safeguards to ensure that the private sector is not coerced into sharing data that might put individuals at risk, or that it is used for purposes outside the scope of the treaty.

¹ This contribution focuses solely on the topics for which treaty text must be submitted by states by 1 July 2022. For the other issues, we contributed in March 2022 a first submission (covering General Provisions, Criminalization, Procedural Measures and Law Enforcement).

² For inspiration, in the Budapest Convention, while electronic evidence is included within the same section, clauses on extradition relate only to the crimes listed in the convention (Articles 2–11).

³ The Budapest Convention provides the most enhanced framework for international cooperation on cybercrime upon which these provisions can be based.



4. Engagement between parties seeking to cooperate should be technical and based on reciprocity. The AHC could consider an efficient and responsive clearing house for requests, which could be hosted by a neutral international organization, or modelled on the 24/7 contact point system used by the parties to the Budapest Convention.

5. Engage civil society for accountability and oversight. All elements of civil society can play a vital role in highlighting new trends and data, and in ensuring international cooperation provisions adhere to human rights standards. The role of civil society groups should therefore be enshrined in this section, setting out how civil society can provide independent advice to states parties and the secretariat.

2. TECHNICAL ASSISTANCE

This process is an opportunity to improve technical assistance support to countries that need it most. This section of the potential convention provides a rare opportunity for consensus in discussions on cybercrime in multilateral settings: technical assistance is provided by numerous international organizations, and is recognized as a need by states across geopolitical divides. However, human rights safeguards need to be reinforced, otherwise there is a risk that states will crack down on legitimate actors, such as journalists and whistleblowers. This section also provides an opportunity to prevent duplication of efforts across the multilateral system.

We offer the following contributions as states consider provisions on technical assistance:

1. Resources should be directed at increasing capacity of law enforcement alongside judicial systems. These should focus on investigation and litigation, but also upholding key rule-of-law principles. They should be reviewed and in line with human rights standards, including through the active engagement and oversight of the Office of the High Commissioner on Human Rights and civil society.

2. Transparency for capacity building is necessary from the beginning. Capacity building can include skills training, legal training, or training in new technological tools. Some states have made clear their interest is for new technologies and capabilities. This treaty should mandate the UN and other international agencies to build capacity for states in a fully transparent way. Attention should be paid to how to safeguard against overreach and build it into the treaty through policies and mechanisms that are actionable.

3. Technical assistance has broad impacts beyond the technical. Technical assistance sets new norms, establishes new or improved powers for the state, and has impacts on communities, particularly in the Global South, where most capacity-building efforts happen through the UN. Activities should be designed and implemented in a way that improves transparency for all. Provisions should include commitments to include outside expertise in capacity-building programmes, including academia, researchers and civil society.

4. Pay attention to prevention. Broader technical assistance approaches should include building the capacity of civil society and communities to better raise awareness of and prevent cybercrime, and respond to it as part of whole-of-society responses.



3. PREVENTIVE MEASURES

The objective for this convention for prevention should be to provide a platform for exchange of information and expertise, which can feed into the technical assistance programmes.⁴ We offer the following contributions:

- 1. Preventive measures are integral to the success of the purposes of the convention as a whole; they are not a separate strand of work.** In particular, preventive measures should form a core part of technical assistance programmes, ensuring that whole-of-society prevention efforts can be identified, refined and replicated.
- 2. Effectiveness of prevention depends on partnerships.** Prevention campaigns depend on the expertise and inputs of private sector, academia and civil society. Therefore, a partnership approach to prevention should be enshrined in the treaty's provisions.
- 3. Foster ongoing exchanges of expertise and best practice.** The convention should allow for the ongoing exchange of information and expertise using the convention and its mechanism of implementation as a platform.

4. MECHANISM OF IMPLEMENTATION

Diplomats working on organized crime at the UN already face a complex and busy set of meetings and processes. Drafting a new implementation mechanism is an opportunity to promote efficiency and innovation, by rethinking and improving on the established review mechanisms of UN treaties such as the UNCAC and UNTOC, which were designed primarily as intergovernmental and legalistic tools, with only limited room for engaging non-state actors or discussion of the broader substantive issues.

In considering how to design the new mechanism, the following key principles should apply:

- 1. The conference of parties and review mechanism should be open, accessible and flexible, and enable discussion of the latest research, trends and data.** This is needed to respond to the changing nature of cyber-related crimes, and to learn lessons from existing crime related treaties – where opaque and bureaucratic mechanisms have led to a limited understanding of implementation.
- 2. The mechanism should enable the most effective capacity building and technical assistance.** To support the delivery of effective and efficient capacity building and technical assistance, it needs to be based on the latest evidence, data and best practices, and ensure engagement with civil society, academic and private sector expertise.
- 3. Go beyond 'on paper' implementation of legal provisions, and consider the impact of the measures taken.** This instrument needs a review mechanism that measures the impact of relevant interventions, in as broad a sense as possible.
- 4. Utilize, and align with, existing multilateral structures and processes.** To amplify the impact of this process, the mechanism should be coordinated and strategically aligned or deconflicted with existing UN processes on transnational organized crime, digital governance, sustainable development and human rights.

⁴ The UNTOC and UNCAC provide extensive examples of prevention provisions that could be used for inspiration in the drafting of this treaty.



RECOMMENDATIONS FOR REVIEW MECHANISM LANGUAGE

This negotiation offers an opportunity to consider a new model for evaluating the performance of legal instruments, and exchanging best practice and expertise through expert-led discussions. With this in mind, we offer the following suggestions for treaty language, inspired by Article 28 of the UNTOC and the modalities and working practices of the AHC:

- 1.** A mechanism of implementation shall be created with the purposes of:
 - a. Analyzing, in a consultative process including states parties and multi-stakeholders, trends in cybercrime/crimes included in this treaty, the circumstances in which they take place, and the actors and technologies involved in committing such crimes.
 - b. Building trust and fostering engagement between states parties, and between states parties and multi-stakeholders as part of efforts to implement the international cooperation provisions of the treaty.
- 2.** The mechanism shall facilitate the development and sharing of analytical expertise concerning cybercrime/crimes included in this treaty amongst states parties and multi-stakeholders.
- 3.** As part of the mechanism, states parties and multi-stakeholders shall monitor the policies and measures put in place by states parties to implement the treaty and make assessments of their effectiveness and efficiency.
- 4.** Capacity building and technical assistance delivered to implement the treaty shall be informed by the data and evidence shared under the auspices of the mechanism.
- 5.** The mechanism shall consist of regular meetings to take place as part of existing meetings of the UN system, for example the UN Commission on Crime Prevention and Criminal Justice, the Conference of Parties to the UN Convention against Transnational Organized Crime, the UN Congresses on Crime Prevention and Criminal Justice, the 3rd Committee of the UN General Assembly, and the Human Rights Council. Meetings shall also take place in varied locations as to enable regional best practice and perspective to be shared – for example as part of meetings of relevant regional multilateral organizations.
- 6.** The mechanism shall have a flexible timetable and agenda to enable it to respond to the latest challenges and issues.
- 7.** In meetings under the auspices of the mechanism, discussions shall be non-political and expert-led.
- 8.** The mechanism shall have a regionally balanced organizing committee or bureau.
- 9.** The modalities for multi-stakeholder engagement in place for the AHC shall apply to the mechanism of implementation, with regular calls for new multi-stakeholders to apply to attend meetings of the mechanism.



5. PREAMBLE AND FINAL PROVISIONS

A preamble should set out a positive rationale for the treaty and what greater purpose(s) it serves, with the following principles in mind:

- 1. A preamble should avoid dramatic statements or assertions and should draw from existing UN language as much as possible,** referencing relevant instruments and couching it within the three pillars of the UN: Human Rights, Peace and Security, and Development.
- 2. There should be a clear recognition of human rights law,** including the Universal Declaration of Human Rights, particularly Article 19, and the International Covenant on Civil and Political Rights.





**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

© 2022 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, CH-1202
Switzerland

www.globalinitiative.net