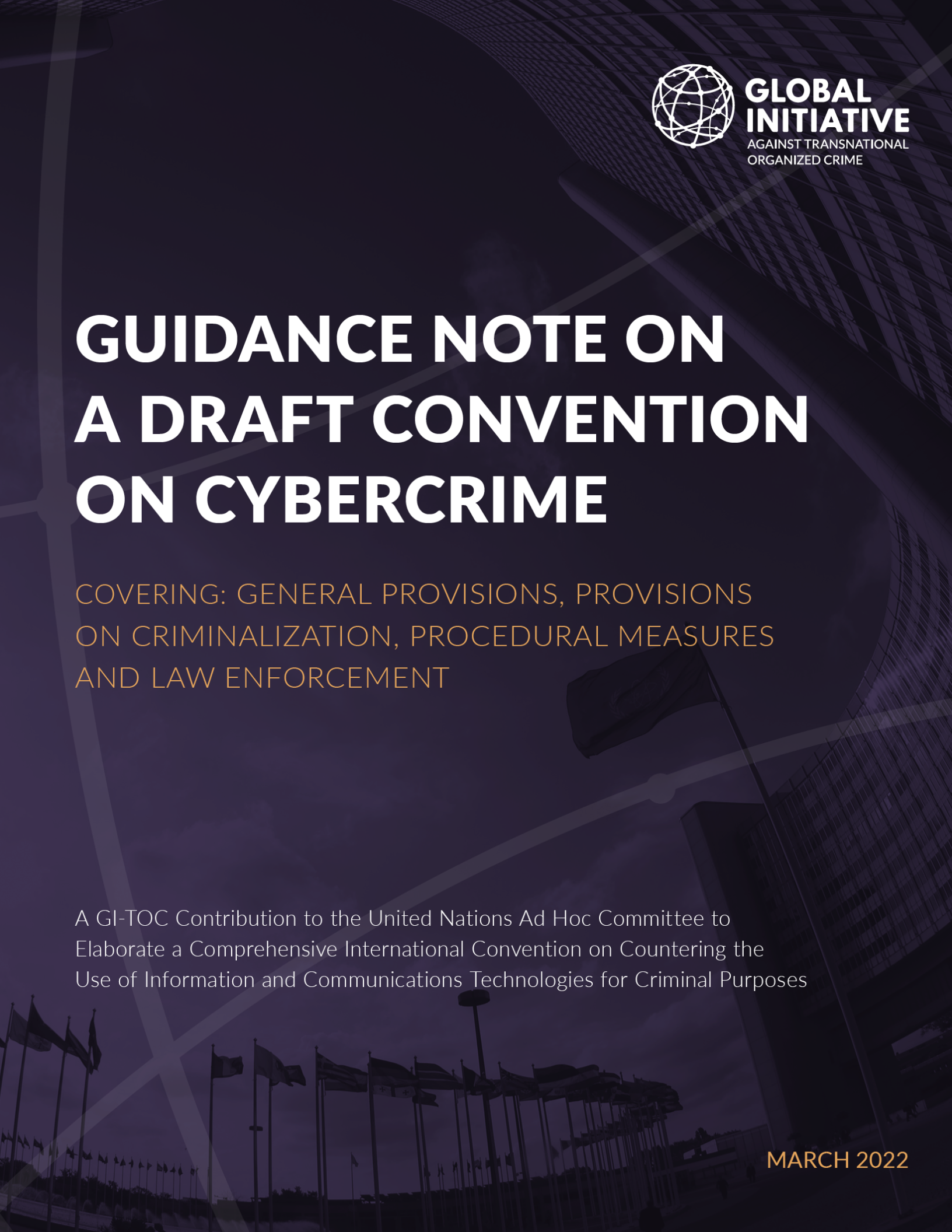

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

GUIDANCE NOTE ON A DRAFT CONVENTION ON CYBERCRIME

COVERING: GENERAL PROVISIONS, PROVISIONS ON CRIMINALIZATION, PROCEDURAL MEASURES AND LAW ENFORCEMENT

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

MARCH 2022

INTRODUCTION

The formal process at the United Nations to negotiate a global cybercrime convention began in 2022. By 8 April 2022, countries must submit their substantive contributions and proposed text on General Provisions, Provisions on Criminalization, Procedural Measures and Law Enforcement. This will be reviewed by the Ad Hoc Committee (AHC) and contribute to proposed treaty language for the 'first reading' of the convention at the second meeting of the AHC beginning on 30 May 2022.

The AHC held its initial meeting from 28 February to 11 March 2022 and revealed varying expectations and positions among members states. The AHC then held its first multi-stakeholder intersessional on 24–25 March. 'Multi-stakeholder' (i.e. private sector, civil society, academia) contributions are vital to ensuring a comprehensive negotiation process informed by a broad spectrum of expert opinion. This again showed a range of positions among participants. Both meetings revealed that states and multi-stakeholder participants are just warming up to this process, exploring the purpose and parameters of the proposed instrument.

In this document, we consider General Provisions, Provisions on Criminalization, Procedural Measures and Law Enforcement, and offer ideas for consideration when drafting language for this treaty. This contribution focuses solely on the topics for which treaty text must be submitted by states by 8 April 2022. For the other issues, we will contribute a second submission (covering international cooperation, technical assistance and capacity building, and prevention).

1. General provisions

'General Provisions' is used in the UN Convention against Corruption (UNCAC), containing articles including purpose, definitions of terms, scope and sovereignty. Given these are typical articles in the UN Convention against Transnational Organized Crime (UNTOC) as well as the illicit drug conventions, we will assume these are the types of provisions that would be included.

1. **The purpose should focus on improving international cooperation (including multisectoral cooperation) to prevent and counter cybercrime.** It should avoid overly ambitious goals (given the scale and ubiquity of cybercrime) or highly political goals (given political tensions around certain issues). This purpose is beneficial, as broader interpretations of the purpose could find governments in disagreement. This would reflect the language of the UNTOC,[1] which could serve as agreed-upon UN language.

2. **The scope should be specific and targeted.** The scope should remain limited and based on an agreed general purpose for the instrument. It should avoid language that is open to interpretation. It could include enhanced international cooperation, combating and preventing cybercrimes as set forth in the treaty, and improving state capacity in partnership with key stakeholders: private sector, academia and civil society.

[1] See UN Convention Against Transnational Organized Crime (UNTOC), United Nations, 2004: 'The purpose of this Convention is to promote cooperation to prevent and combat transnational organized crime more effectively.'

3. Definitions should be concrete and, where possible, based on existing agreements. There needs to be clarity and shared agreement on the definitions used in the treaty. Definitions for crimes addressed under the convention should be provided in the section on criminalization. Given the title of this process, an agreed upon definition of ICT should be given here, and of cyber-dependent and cyber-enabled crime.

4. The general provisions should contain rights safeguards in terms of what the convention should not criminalize or instrumentalize for international cooperation. There is a risk that focusing on content-related activities deemed criminal in some countries could restrict freedom of speech and other rights online. This point was discussed at the AHC's first meeting, including by a number of non-governmental organizations that participated in the meeting and have publicized their views in public documents. The instrument must steer clear of creating opportunities to restrict human rights and fundamental freedoms, and should clearly state this principle.

5. Benefits of technology should be recognized alongside harms caused by cybercrime to people, societies, economies and the environment. The general provisions could reiterate that information and communication technologies (ICT) and the internet are global goods and form part of our social and political fabric, and are key to achieving the Sustainable Development Goals. A convention could thus be framed as protecting these utilities for all citizens, while protecting potential victims of cybercrime.

6. Promote UN system-wide coherence. The general provisions section could address coherence. In the UNTOC protocols there is an article, *Relation with the United Nations Convention against Transnational Organized Crime*, which defines how they relate to one another. One regular criticism of UN instruments, including those in the criminal justice sphere, is that they exist as silos without adequate coherence. This instrument could include an article in this regard and lay out how it relates to (1) Universal Declaration of Human Rights Article 19 and (2) to the UNTOC and its protocols.

7. Sovereignty. There is agreed-upon UN language on sovereignty, which it is assumed will form the basis of sovereignty in this treaty. Cross-jurisdictional storage of and access to data are key areas of divergence among states, yet these are unlikely to be addressed in the 'general provisions' section.

Note on process: If general provision language is so contentious that it is taken to a vote for approval, it is unlikely the treaty will achieve widespread and diverse adherence.

2. Provisions on criminalization

The criminalization section is key to the treaty's role in establishing norms. 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 might be 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 scope of criminal activities in this section are therefore critical. It is extremely hard to undo what has been written into a treaty rather than adapt and update it through resolutions. For that purpose, we caution strongly against listing a series of cyber-enabled crimes (i.e. existing crimes exacerbated by technology), or horse trading between crimes to arrive at an agreed-upon list.

1. The instrument should focus primarily on cyber-dependent crimes. Within existing frameworks (e.g. the Budapest Convention), there is established cooperation for these types of crimes. However, between regions and countries without shared agreements, cooperation in prevention and investigation of cyber-dependent crimes remains weak and often impacted by geopolitics. Member states disagree strongly on cooperation for crimes that might impinge on online freedoms, private enterprise, and political and free speech. Negotiations would miss an important step if they assume cyber-dependent cooperation is a given and move on to debating cyber-enabled or content-related crimes. Cyber-dependent crimes impact public and private entities and infrastructure, and individuals – victims come from across society. Achieving broad international support for norms and mechanisms for cyber-dependent crimes would be a positive achievement and a measure of success for this process.

2. Avoid duplicating criminalization of acts addressed in other protocols and treaties. Some cyber-enabled crimes (e.g. cyber-enabled human trafficking) could be addressed through provisions of the treaty, but not under criminalization. The challenges in preventing, investigating, detecting and prosecuting these types of crimes should be addressed under technical capacity, international cooperation and procedural measures. Many of these acts are already criminalized or addressed through existing legislation. And there may not be a legislative or substantive need to create a new framework to address them. Therefore, the instrument should build on, and not 'reinvent', what already exists in regional and UN instruments.

3. Crimes should be concrete, based on existing agreements, and focused on criminal activities that materially impact victims, and not crimes against the state. There should be certainty on the scope of potential crimes that are covered by the treaty. Unlike the UNTOC, a benefit of which is flexibility of types of transnational organized criminal activity that fall within it, clarity is needed for this instrument. This is due to the widely divergent views of member states on what constitutes crimes online, and potential harms that could be caused. It should not promote definitions of cybercrimes as crimes against the state. And the treaty should not be used as a platform or mechanism to criminalize journalism, information sharing, activism, community organization or dissent.

4. List what is outside the scope of the treaty. States could consider listing specific types of activity that are not to be considered cybercrimes under the convention. For example, journalism and whistleblowing could be cited as acts that contribute to peaceful societies and help combat organized criminality.

3. Procedural measures and law enforcement

This convention could build trust between practitioners to foster more effective and cooperative international law enforcement and apply criminal justice responses to cybercrime. The treaty could achieve this by (1) assigning cross-border cooperation at the level of judicial and law enforcement cooperation; and (2) by not defining cybercrimes as crimes against the state, particularly any content-based crime.

1. The primary relationships to be fostered through the treaty should be bilateral. This section should focus on improving bilateral assistance in investigation and prosecution of cybercrimes under the convention. It should improve all countries' ability to gather and share cross-border evidence and data in a mutually trusting way, prioritizing transparency. In facilitating this cooperation, there should be adequate safeguards on human rights, privacy and data protection, protection of witnesses, including whistleblowers and journalists.

2. Encourage multi-sectoral cooperation. The instrument should not only enhance practical cooperation between law enforcement and the judiciary, but also between law enforcement, the private sector, academia, and civil society. The role of civil society should be enshrined in the convention, recognizing its role in research and investigation, raising awareness, and protecting communities against cybercrime, alongside law enforcement, the private sector and other stakeholders.

3. Address the role of the private sector. This is a convention to be agreed between states, but the key role of the private sector as part of law enforcement and procedural measures should be addressed. Although there is limited appetite to create new regulations or restrictions on the technology sector at the multilateral level, and states have such varied domestic regimes and relationships to their companies, it is nevertheless essential to provide some guidance in the treaty, if specific frameworks or mechanisms for data and evidence sharing cannot be agreed on. For example, the instrument could address the role and responsibilities of the tech providers and social media platforms in preventing and responding to the criminal activity within the scope of the treaty. This should be done in the spirit of trust-building and transparency that help foster the bilateral relations needed to implement any convention effectively.

4. Protect victims, witnesses and whistleblowers. While promoting law enforcement cooperation and procedural measures, protection of victims, witnesses and whistleblowers should also be prioritized. The instrument could reiterate and build upon relevant UNTOC provisions, including Articles 24 and 25, which oblige states to provide protection for witnesses from 'retaliation or intimidation', including for their relatives or others close to them, and to provide assistance and protection for victims, including compensation and restitution. This section could include innovative ways of responding to the rights of victims in the digital age, as witnesses and whistleblowers face novel ways of being threatened, intimidated or extorted using online means.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

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

www.globalinitiative.net