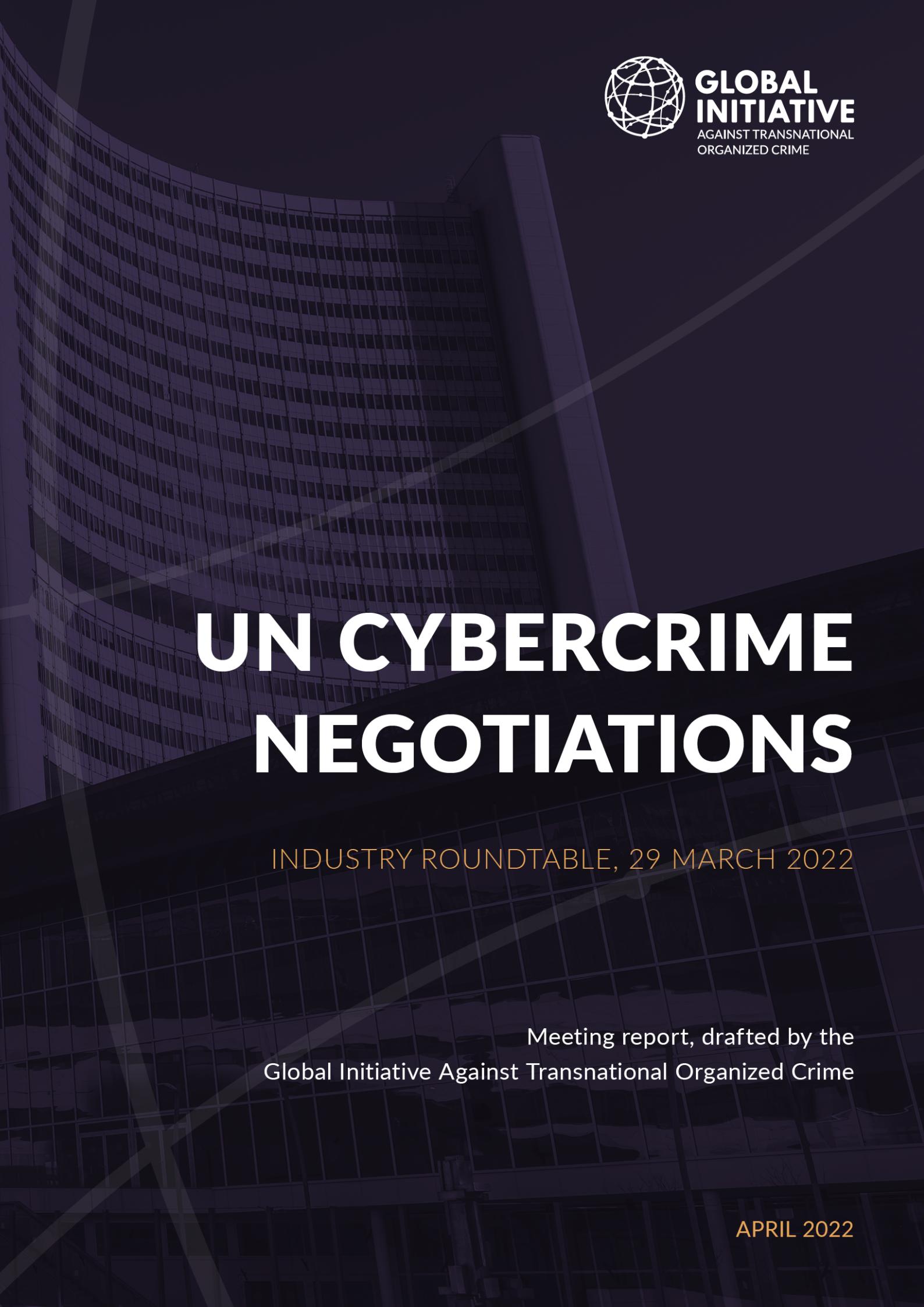

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

UN CYBERCRIME NEGOTIATIONS

INDUSTRY ROUNDTABLE, 29 MARCH 2022

Meeting report, drafted by the
Global Initiative Against Transnational Organized Crime

APRIL 2022

INTRODUCTION

As part of a collaboration between the UK government and the Global Initiative Against Transnational Organized Crime (henceforth 'GI-TOC') to promote civil society engagement in the UN negotiations around a cybercrime treaty, the GI-TOC organized a meeting to consult key experts and industry stakeholders. The purpose was to provide inputs for the UK government as it develops its submissions and negotiating positions for the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (henceforth the 'Ad Hoc Committee').

The event was designed to allow the UK government to hear the perspectives and positions of industry stakeholders and members of the GI-TOC Network of Experts on key elements of the proposed legal instrument, to be later discussed in official negotiation sessions at the UN. The issues addressed in this roundtable aligned with the topics states are due to address in the Ad Hoc Committee's second session: criminalization, the general provisions, and the provisions on procedural measures and law enforcement. Issues related to prevention of cybercrimes were also covered.

The UK government opened the meeting by highlighting their interest in hearing multi-stakeholder inputs as the treaty negotiations advance, noting that for the treaty to be effective and practical, it needs to be informed by multi-stakeholder input. The UK government also underlined the importance of having gender and human rights considerations in the convention's objectives and scope, and requested stakeholders' views in specific areas, such as Child Sexual Abuse Material (CSAM), data sharing and corporate responsibility.

In its opening remarks, the GI-TOC provided background on the treaty negotiations and informed participants about the latest updates on the negotiation process.

Topic 1: General objectives and scope of a convention

This session presented the perspectives of participants on what the focus of the treaty should be with regard to its general provisions, such as the purpose of the convention, definitions, scope and sovereignty.

Narrow scope and approach. Notwithstanding some scepticism raised by the private sector, participants generally agreed on the need for some kind of improved legal framework or a convention due to the nature of the challenge posed by cybercrime. Overall, the group sensed that definitions should be clearly stated, and that the scope should include references to what the convention does and does not cover. The group favoured adopting a narrow approach that excludes cyber security dimensions and builds upon existing instruments. Participants stated the need to make robust reference to human rights, data protection and the right to privacy. On private sector regulation, the private sector was cautious and some participants said that industry regulation should not be a part of the treaty.

Participants asked whether this convention could be an opportunity to create a mechanism to deal with so-called safe haven nations. It was noted that cooperation should be the aim, but some questioned how this could be feasible when some governments currently block cross-border investigations. Participants questioned whether a global instrument could sit with this dynamic.

Whole-of-society approach. On the objectives of the convention, two ideas were raised by participants. One is that the convention should provide a framework that supports a whole-of-society approach to tackle cybercrime. References were made to international cooperation, public-private cooperation and national cooperation. Concerns were raised about the lack of an enforcement mechanism when it comes to inter-state cooperation, with the hope that a global instrument would address this.

Criminal justice focus. Participants expressed the need for a criminal justice instrument and that cooperation should be designed to foster intelligence-led approaches, and information sharing to allow for prosecution. Participants emphasized the need to be mindful when providing law enforcement capacity building of not undermining human rights standards or obligations.

Topic 2: Provisions on criminalization

In this session, participants were asked to discuss their views and practical considerations from the perspective of the private sector and civil society. Participants expressed their concerns about the misuse of cybercrime laws by governments. They flagged risks for the security of researchers, investigative journalists and broader civil society. The risks to security analysts was a particular point raised by several participants, and it was felt that these communities should be properly empowered and acknowledged in the text of the convention, and that careful consideration will need to be given to the risks of human rights violations while drafting the convention.

Participants were supportive of using the Council of Europe Convention (the Budapest Convention) as a baseline for criminalization provisions. Some pointed to the limitations of the Budapest Convention, saying that the future cyber treaty should go beyond it. One participant, for example, highlighted the practical difficulty of distinguishing between authorized and unauthorized use, specifically for private actors conducting investigative work. It was also noted that not all states are party to the Budapest Convention, and regional perspectives should be taken into account. Due to this diversity of regional perspectives, participants reinforced the need for a clearly defined crime-focused criminal justice treaty to avoid the instrument straying into more complex and politically challenging issues of cyber security.

Participants agreed on the inclusion of cyber-dependent crimes but diverged on the inclusion of cyber-enabled crimes. Overall, participants seemed to be in line with the inclusion of cyber-dependent crimes in the treaty. However, and inevitably, the discussion on criminalization led to the question of whether and how to include cyber-enabled crimes. One participant suggested the criteria for which crimes to include in the treaty should be based on what is not covered in other treaties. This could be a way of limiting the potential overreach of the scope of the criminalization provisions. The participants were very cautious about the pitfalls of including a list of crimes and reiterated the need for the convention to be a 'living document' that can be used when future technologies emerge. However, crimes related to child sexual abuse material were broadly recognized as crimes that should be dealt with by the convention.

On content-related crimes, divergence in regional perspectives was noted as a considerable challenge. Participants recognized differences between countries in terms of their culture, values and social norms, which would make approaches to content-related crimes unmanageable.

Some definitions of crimes were proposed by participants. One was that cybercrime could be defined as crimes directed at computers or other information communications technologies (ICTs) and where computers or ICTs are an integral part of an offence. Another proposal was to distinguish between crimes between 'crimes against property' and 'crimes against the person'. These was seen as an option that would exclude crimes against the state.

Topic 3: Law enforcement and procedural measures

In this section, participants were asked to discuss their views and provide practical considerations, challenges and opportunities that could be reflected in provisions on law enforcement and procedural measures. There was a general understanding that the treaty should include measures to boost investigative capacity and provide tools to enable prosecutions of the crimes to be covered by the treaty. At the same time, participants were mindful that this is an area that requires a cautious approach, and proper guidelines and constraints should be included in the provisions. According to the participants, a balance should be struck in the wording of the treaty between the interests of law enforcement and respect for fundamental human rights.

Access to and sharing data and e-evidence. Regarding data collection and sharing, participants cited the challenge of collecting data across different jurisdictions. While some recognized the need for a standardized mechanism to request data, this would not come without hurdles. A point reiterated by many participants is that requirements for the disclosure of data on individuals should be designed in line with human rights standards and to avoid abuse.

Private sector participants raised concerns regarding compliance. While in some regions data protection has higher safeguards, in others the threshold for sharing data is lower, which makes it very difficult for companies to comply with conflicting requirements between governments or with requirements that that might undermine the human rights or privacy of customers.

Another concern for private sector participants was over whether onerous costs would be created for corporations. The private sector participants believed that the treaty should not allow for bulk information sharing, should identify the types of data to be shared and should provide a channel for challenging government requirements. Requests should be limited and based on principles of proportionality and necessity.

Ideas were shared around including cyber-enabled crimes, such as CSAM, in cooperation measures. Reasons given were based on the challenges cyber-enabled crimes present to traditional law enforcement investigations and processes.

The need to look at the full cycle of data use during investigations and prosecutions. One of the challenges mentioned by participants is how to ensure that e-evidence is acceptable before different national courts. The means by which law enforcement might be permitted to obtain evidence differ from country to country, and this might make e-evidence inadmissible before courts in certain jurisdictions. Time delay has also been an issue in cross-border investigations, and this was raised in the meeting.

Jurisdiction and international cooperation – public-private partnership as key. Some participants said that jurisdiction should be attributed according to territorial and sovereignty criteria, and language on extraterritoriality should be avoided. However, standards for international cooperation as part of the new treaty were a shared priority among participants.

Partnership and engagement with the private sector was highlighted specifically in areas of developing projects that could create best practices and the fight against CSAM. Experts on CSAM outlined the need for the private sector, specifically financial companies, to understand their role in preventing acts such as dissemination and livestreaming through awareness raising. Another area for potential collaboration was in handling the volumes of data that are normally attached to these cases. Here, the private sector can help law enforcement triage and prioritize when refereeing data material.

De-escalating cooperation from the geopolitical. One discussion point was the role of organizations such as INTERPOL and the UNODC in helping overcome political barriers to cooperation and providing support with capacity building. A multilateral agreement with strong, impartial guidelines on law enforcement can help mitigate political considerations that hinder investigations. Participants acknowledged that INTERPOL can play an important role in dissemination of information. However, they had reservations on including specific organizations, as this would risk limiting the provisions of the convention. A more favourable approach, it was suggested, would be for the convention to provide certain specific roles in the context of international cooperation, capacity building and sharing of information, without naming specific organizations or bodies.

Topic 4: Prevention

Prevention is one of the most cross-cutting areas to be addressed by the proposed treaty. Participants discussed what would constitute effective examples of preventive activity to be included in the treaty, as well as ineffective approaches that should be avoided.

Prevention is fundamental as part of any global effort to make cybercrimes more difficult to commit. It was clear that participants thought that preventive measures should be reflected in laws or policies dealing with cybercrime. Participants highlighted two different areas of focus on prevention. Firstly, participants highlighted the interconnection of prevention with deterrence – states have an obligation to prosecute actors carrying out crime in order to deter others. Secondly, prevention requires skills building, and therefore the convention should have heavily emphasize capacity building. It was also recommended that the convention include language that encourages research and investigative work focused on prevention.

Need for awareness raising and education. Participants agreed that civil society, academia and other groups in partnership with the private sector have an important role in enhancing preventive activity. Activities should focus on raising awareness and educative tools – in particular, educating school-age children was raised as a priority. Research innovation and association with academia and civil society were also suggested. The instrument could support a forum for ongoing exchange involving civil society, academia and the private sector as part of a review mechanism. A static convention with no follow-up was not advisable, it was thought.

CONCLUSIONS

There was a general agreement that the convention's objectives and scope should be succinct, clear and avoid overreach. It was also voiced that the treaty should make a clear reference to human rights and fundamental freedoms. On criminalization, participants supported the inclusion of cyber-dependent crimes in the convention, but diverged on whether, and how, to include cyber-enabled crimes.

On law enforcement and procedural measures, participants mentioned obstacles to cooperation, including cross-border investigations, political barriers and concerns from the private sector on how to comply with states' requests while protecting the rights of their customers. The role of intergovernmental actors was highlighted in cooperation and capacity building as well as the need to ensure that treaty implementation would be a dynamic process. On prevention, strong capacity building, education, skills, and disincentive and deterrence to committing crimes were key elements mentioned by participants.

ANNEX 1:
DOCUMENTS SHARED IN THE MEETING

- Draft Convention on Electronic Evidence, https://journals.sas.ac.uk/deeslr/article/view/2321/2245
- UK CLRNN research on national legal frameworks that include protections for security researchers, http://www.clrnn.co.uk/media/1028/clrnn-1a-comparative-report-on-computer-misuse-defences.pdf

ANNEX 2:
AGENDA

Time	Agenda item	Objective
13:00–13:10	**Opening session**	Welcome: Virginia Eyre, Deputy Director Cyber Policy, UK Home Office, Ian Tennant (GI-TOC) Roundtable introductions
13:10–13:45	**General Provisions: General objectives and scope of a convention**	Moderator: Summer Walker (GI-TOC) Introduction of the issues Discussion to solicit views and practical considerations Challenges and opportunities participants envisage from the perspective of the private sector
13:45 – 14:30	**Provisions on Criminalization**	Moderator: Summer Walker (GI-TOC) Introduction of the issues Discussion to solicit views and practical considerations Challenges and opportunities participants envisage from the perspective of the private sector
Break (10 minutes)		
14:40–15:25	**Procedural Measures and Law Enforcement**	Moderator: Ian Tennant (GI-TOC) Introduction of the issues Discussion to solicit views and practical considerations Challenges and opportunities participants envisage from the perspective of the private sector
15:25–16:05	**Prevention**	Moderator: Ian Tennant (GI-TOC) Introduction of the issues Discussion to solicit views and practical considerations Challenges and opportunities participants envisage from the perspective of the private sector
16:05–16:15	**Closing session**	Initial conclusions Closing remarks: Virginia Eyre, Deputy Director Cyber Policy, UK Home Office

ANNEX 3:
PARTICIPANTS

Category	Name and position
UK government	Virginia Eyre, Deputy Director Cyber Policy, UK Home Office Representatives from UK Home Office and Foreign, Commonwealth and Development Office
GI-TOC staff and experts	Summer Walker, New York Representative and Senior Analyst, GI-TOC Ian Tennant, Head of Vienna Multilateral Representation and Resilience Fund, GI-TOC Ana Paula Oliveira, analyst, GI-TOC Karl Lallerstedt, Senior Advisor Security Policy, Confederation of Swedish Enterprise Tariq Khosa, Director Centre for Governance Research, Pakistan Bindu Sharma, Managing Director, Asia Pacific, International Centre for Missing & Exploited Children Crispin Yuen, Director, AML Sanctions Malina Enlund, Trust and Safety Manager APAC, Facebook Mauricio Bastien Olvera, Cybercrime Lecturer, National Autonomous University of Mexico
Sector Stakeholders	Katharina Sommer, Head of Public Affairs, NCC Group Daniel Aldridge, Senior Policy Manager, BCS, The Chartered Institute for IT Michael Tunks, Senior Policy and Public Affairs Manager, Internet Watch Foundation John R. Hering, Senior Government Affairs Manager, Microsoft Corp. Shaun Holt, Group Leader, STERG