18 November 2022

English only

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
Fourth session
Vienna, 9–20 January 2023

Chair's Report of the Third Intersessional Consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Note by the Secretariat

1. The present text was prepared by the Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. It contains the Chair's report of the Third Intersessional Consultation, held on 3 and 4 November 2022.

2. The Third Intersessional Consultation of the Ad Hoc Committee was held in accordance with paragraph 10 of General Assembly resolution 75/282, in which the General Assembly encouraged the Chair of the Ad Hoc Committee to host intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention, the modalities of the participation of multi-stakeholders in the Ad Hoc Committee, contained in Annex II of the report of the session on organizational matters (available here), as well as the road map and mode of work for the Ad Hoc Committee contained in Annex II of the report of the first session of the Ad Hoc Committee (available here).

3. The Third Intersessional Consultation was held in English over four meetings in Vienna and online (the agenda is available here). It was attended by representatives of 61 multi-stakeholders: 6 from United Nations bodies, specialized agencies, funds and functional commissions of the Economic and Social Council, 4 from intergovernmental organizations, 21 from non-governmental organizations in consultative status with the Economic and Social Council and 30 from other non-governmental organizations, civil society, academic institutions and the private sector. The consultation was also attended by 68 Member States and non-member observer States.

4. The intersessional consultation was chaired by H.E. Ms. Faouzia Boumaiza Mebarki (Algeria), Chair of the Ad Hoc Committee, and Mr. Eric Do Val Lacerda Sogocio (Brazil), Vice-Chair of the Ad Hoc Committee.

5. A panel discussion was held under agenda item 2, entitled "A balancing act: human rights considerations in the drafting of the chapters on general provisions, criminalization and procedural measures and law enforcement of the draft convention on countering the use of information and communications technologies for criminal purposes", with presentations by Mr. Tim Engelhardt, Human Rights Officer at the Office of the United Nations High Commissioner for Human Rights, Mr. Ashok Yende, President of Global Vision India Foundation, Ms. N.S. Nappinai, Founder of the Cyber Saathi Foundation and Ms. Katitza Rodriguez, Policy Director for Global Privacy at Electronic Frontier Foundation.

6. The panellists addressed a variety of human rights considerations to be taken into account when formulating the substantive and procedural provisions of the future convention. The first panellist emphasized that law must be carefully drafted in accordance with the principles of legality, legitimate aim, necessity, and proportionality. He cautioned against overly broad provisions that could be used against political opponents, human rights defenders and journalists and could violate human rights and fundamental freedoms. He further highlighted that the convention should focus on core cybercrimes and exclude content-related crimes from its scope. He also stressed that the convention should make the essential requirements and safeguards for the investigative measures needed to fight cybercrime mandatory. In relation to provisions on international cooperation and the dual criminality requirement, he noted that the future convention must ensure that domestic human rights protections cannot be circumvented. The second panellist stressed that the proposed treaty should be consistent with existing United Nations international conventions in this area, which apply to most States. She called for an expanded scope of the convention which, in addition to cyber-dependent crimes, would include a list of cyber-enabled crimes. The third panellist underscored the need for drawing the boundaries and ensuring checks and balances in relation to the use of information and communications technologies for criminal purposes. She also noted the importance of balancing human rights with law enforcement needs to ensure that the future convention provides an effective platform for law enforcement cooperation and addresses territoriality concerns. Furthermore, she suggested that the future convention should contain provisions on users' duties, as well as the liability of corporate entities. The fourth panellist focused on safeguards against the abuse of law enforcement powers. She proposed that the preamble of the convention refer to the existing human rights standards and acknowledge that all human rights that apply "offline" should also be afforded and protected online. She urged the meeting to recognize that restrictions on the use of anonymity and encryption could conflict with human rights and fundamental freedoms. Moreover, she emphasized that to avoid abuse, access, use and collection of data should be based on the principles of legality, necessity, proportionality, be narrow in the scope of application and based on judicial authorization.

7. Following the presentations, the Chair of the Ad Hoc Committee opened the floor for questions and statements by multi-stakeholders, Member States and non-member observer States. In response to the question of whether it would be sufficient for the draft convention to refer to the existing international legal framework on human rights, it was emphasized that the existing international legal framework on human rights provides a strong foundation and is flexible to face the challenges posed by the use of information and communications technologies for criminal purposes. Concerning the question on the inherent tension between the choice to either reinforce or improve human rights standards in the convention, several speakers stressed that it would be possible to do both by guaranteeing that the convention refer to the existing international legal framework while ensuring, for example, the implementation of these obligations. In addition, several speakers noted potential challenges in drafting the convention considering that human rights

obligations differed in each State. Subsequently, the consideration of a minimum standard for provisions on the protection of human rights and fundamental freedoms to be followed by the convention was proposed, with a view to ensure strong protections as well as a consensus-based approach. In particular, when discussing how best to include human rights safeguards in the convention, some speakers voiced support for a practical approach by having Member States first agree on a common set of international human right obligations to be explicitly mentioned in the convention, in an as robust as possible manner, and then consider which additional protections might be needed. Furthermore, several speakers reiterated the importance of the principles of legality, necessity and proportionality in any procedural powers given to law enforcement agencies in the convention for the investigation of cybercrime. Moreover, the criminalization of misinformation, also known as "fake news", was deemed highly problematic and its inclusion in the convention was strongly discouraged by one of the panellists. In addition, it was highlighted that the convention should be regarded as an opportunity to modernize the United Nations conventions on crime prevention and criminal justice, in particular with regard to electronic evidence, and thus be able to fight cybercrime more efficiently.

8. The discussion under agenda item 3, entitled "Renewed opportunities: the draft convention on countering the use of information and communications technologies for criminal purposes to further strengthen the protection of children", was preceded by a panel with presentations by Mr. Francis Monyango, Research Fellow at Strathmore University, Ms. Amy Crocker, Head of Child Protection and Technology at ECPAT International, Ms. Afrooz Kaviani Johnson, Child Protection Specialist at UNICEF, Mr. Manus de Barra, Child Protection Officer at the Office of the United Nations Special Representative of the Secretary General on Violence Against Children and Mr. LU Chuanying, Senior Fellow at the Shanghai Institutes for International Studies.

9. The first panellist elaborated on the child's right to privacy as an antidote in countering the criminal use of information and communications technologies. He noted that the abundance of children's personal data, shared online by, among others, parents themselves, could infringe on the privacy of children, harm their mental health and physical well-being, and result in economic harms or commercial exploitation. The second panellist stressed the importance of taking child rights-based approach in negotiating the provisions of the future convention. She noted that protecting children online was not only a moral obligation, but also a legal obligation under the existing children's rights instruments. She also emphasized that divergent terminology and inconsistencies in national laws led to a lack of common understanding that caused challenges for international cooperation and data sharing, which were critical in the detection, investigation and prosecution of such offences. She encouraged the use of consistent terminology, as recommended for example in the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), and inclusive definitions of offences. Furthermore, she proposed to exempt minors, defined as persons under 18 years of age, from prosecution for age-appropriate consensual sexual activity and to remove the requirement of double criminality in relation to online child sexual abuse offences. The third panellist noted that children, besides the risk of being victims of offences enabled by the use of information and communications technologies, may also be accused or convicted of such offences, and thus she underlined the need for a child-friendly justice system, including principles and procedures, separate from the justice system designed for adults. She noted that the future convention could provide renewed opportunities for strengthening children's rights and protections, and expressed the hope that the existing instruments, such as the United Nations Convention on the Rights of the Child and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, would be expressly referred to in the convention. She stressed the importance of setting appropriate criminal sanctions, as well as special measures for child victims and witnesses. The fourth panellist highlighted the importance of child-friendly justice principles to treat children in contact with the justice system as victims or witnesses in a child-sensitive

manner and with due regard to their dignity and needs. He pointed out that crimes facilitated by information and communications technologies and affecting children were not limited to child sexual exploitation and abuse but could also include other types of crime that needed to be addressed, such as abduction, recruitment by armed groups and coercion to participate in criminal activities. He stressed that children coerced to commit crime should be treated as victims by echoing the principle of non-punishment of victims of human trafficking. The fifth panellist presented the findings of a national survey that targeted children between 8 and 12 years of age and aimed at identifying the online risks to which children are exposed. He underscored the important role of parents, educators, civil society and governments in protecting and educating children on cyber risks and cyber safety measures, and in creating a child-friendly digital environment.

10. Following the presentations, the Vice-Chair of the Ad Hoc Committee opened the floor for questions and statements on agenda item 3. Many speakers provided examples of best practices in child-friendly justice settings, especially in relation to the treatment of child victims and witnesses in criminal proceedings. References were made to several reports, analyses and guidelines on justice in matters involving children, including those adopted by the General Assembly. Some speakers noted that child protection was the area in which consensus among States could be reached, and which could serve as a good starting point for international cooperation. Many speakers also emphasized the importance of using consistent and up-to-date terminology and explained that the term "child pornography'' should be avoided, as pornography is associated with consensual sexual activity and children cannot consent in this regard. Furthermore, several speakers agreed that the future convention could seek to raise the bar of child protection standards. Many speakers also acknowledged the crucial role of the private sector, notably large technology companies in preventing and addressing various forms of crime against children and in protecting children's rights. It was stressed that governments should cooperate with the private sector and encourage a culture of safety by design. Several speakers reiterated the need for abolishing statutes of limitations with regard to offences related to child sexual abuse and exploitation, given the many barriers for children to report such crimes. Several speakers suggested making explicit reference to the principle of the best interests of the child not only under criminalization provisions, but also throughout the future convention. It was further noted that significant obstacles exist to grant compensation for victims of child sexual abuse and exploitation. Moreover, it was noted that the sexual exploitation of boys was not always reflected in laws.

11. Under agenda item 4, entitled "The power of words: a discussion on terminology and other aspects of the chapter on general provisions", a panel discussion was held with presentations by Ms. Eun-Ju Kim, Programme Coordinator at the International Telecommunication Union, Mr. Jose Cepeda Garcia de Leon, Spanish Senator and member of the Inter-Parliamentary Union, and Mr. Nick Ashton-Hart, Special Adviser on International Internet Policy at International Chamber of Commerce – United Kingdom.

12. The first panellist recommended the use of technology neutral terminology due to the fast-evolving nature of digital technologies. She referred to the International Telecommunication Union's resolutions and recommendations setting international standards on various types of information and communications technologies and their security. She also encouraged States to consider and utilize those standards when elaborating the future convention. The second panellist emphasized the importance of the regulation of cyberspace to face the challenges posed by cybercrime and to preserve democratic values. He further stated that any restrictions to the content of social networks must be lawful, narrowly defined and enforced under judicial and parliamentary supervision. The third panellist underlined that, while he understood the decision by Member States of discussing the terms of the future convention at a later stage, a consensus on basic terminology and the scope of the future convention would allow the discussions of the convention to move forward smoothly. In this regard, he stressed the need for a common understanding of what constituted crime

for the purposes of applicability of the convention and noted that the convention should apply only to serious cybercrime. Furthermore, in relation to the possibility of the provisions on international cooperation applying to offences beyond those defined in the future convention, the speaker stressed the importance of a minimum threshold to apply the Convention to serious crimes.

13. Following the presentations, the Vice-Chair of the Ad Hoc Committee opened the floor for questions and statements by multi-stakeholders, Member States and non-member observer States. Some speakers recommended the use of the term "cybercrime", as opposed to "the use of information and communications technologies for criminal purposes", considering that the former included criminal acts, while the latter was an overly broad term subject to different definitions in different jurisdictions and could undermine the freedom of expression. Several speakers stressed that the convention should use technology-neutral terms and focus on cyber-dependent crimes. Furthermore, the need was underscored to include offences against persons and property, of which information and communications technologies were an integral part, instead of offences against States. Some speakers highlighted the importance of using definitions taken from other relevant international instruments to the maximum extent possible and to divert from the existing terms only when necessary and unavoidable. In addition, reference was made to the conclusions and recommendations emanating from the Intergovernmental Expert Group on Cybercrime to define the offences in the draft convention. Referring to the application of the future convention to crimes that may not be directly covered by the convention, some speakers emphasized that in order to enable the application of the convention's provisions on international cooperation a concept of "serious crime" should be included. In contrast, with regard to definitions not to be included in the convention, it was recommended to avoid definitions that could inadvertently limit human rights and fundamental freedoms or have unforeseen negative consequences to the application of other relevant international treaties.

14. A panel discussion was also held under agenda item 5, entitled "A concerted effort: the role of the private sector in the context of the chapter on criminalization and procedural measures and law enforcement", with presentations by Ms. Pei Ling Lee, Head of Cyber Capabilities and Cyber Strategy at the International Criminal Police Organization (INTERPOL), Mr. Nemanja Malisevic, Director of Digital Diplomacy at Microsoft, Mr. Farhan Sahito, Director General at Privanova SAS, Mr. Will Hudson, Corporate Counsel at Google Inc., on behalf of International Chamber of Commerce - United Kingdom and, on behalf of the Institute for Security and Technology, Ms. Megan Stifel and Ms. Zoe Brummer, Chief Strategy Officer and Principal coordinator of the Framework for Cyber Incident Reporting respectively.

15. The first panellist, having noted the provisions on law enforcement and private sector cooperation of the existing international instruments, provided an overview of the areas in which INTERPOL successfully partnered with the private sector. These included data sharing, analysis and research, capacity-building (i.e.: training programmes integrating hands-on exercises with real-world simulations leading to real investigations), development of investigation tools and platforms, and operational support (e.g.: transcontinental joint operations facilitated by cyber fusion centres with seconded experts from the private sector). She also stressed the importance of secure communication channels, robust procedural frameworks and data sharing agreements governing public-private partnerships with due regard to the principles and rules for processing of data, as well as international human rights standards. Highlighting the role of the private sector in bridging the gap in technical capabilities and finding innovative solutions to counter cybercrime, she encouraged the widest possible cooperation between law enforcement authorities, private sector and other actors and platforms. The second panellist highlighted an increasingly sophisticated landscape of cyber-attacks and stressed the need for the scope of the future convention to be limited to cyber-dependent crimes and procedural provisions to facilitate cooperation between law enforcement authorities and the private sector. He encouraged the use of relevant provisions of the existing international instruments,

such as the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and the Council of Europe Convention on Cybercrime, to the maximum extent possible noting that introducing different provisions could lead to unintended results. He also stressed that the provisions of the future convention should facilitate international cooperation between public and private sectors, while ensuring confidentiality, integrity and availability of data, safeguarding against human rights violations and providing for legal redress mechanisms. The third panellist referred to the increasing volumes of cyber-attacks and the limited resources and capabilities of law enforcement authorities to tackle them and underscored the importance of strong public-private partnerships in the fight against cybercrime. Furthermore, he briefed the meeting on the reasons for the underreporting of cybercrime in the private sector, including lack of resources and perceived negative consequences for businesses. He also emphasized that to foster public-private partnerships, the regulatory frameworks should stimulate and facilitate the reporting of cybercrime by striking a balance between penalties and incentives for private sector companies, while considering their needs. The fourth panellist underlined the unique perspectives and experiences of the private sector in tackling cybercrime because of how it affected its users and platforms. He noted that the future convention should avoid exacerbating the conflict of laws governing data disclosure requests and could do so by focusing on serious cyber-dependent crimes and providing for a dual criminality requirement applicable to international cooperation in relation to procedural measures. He also emphasized that human rights protection should be at the core of the future convention. The fifth and the sixth panellists focused on best practices for cyber incident reporting frameworks, especially by medium-sized entities. They underscored the need for simplified (e.g.: “one-stop-shop”) and harmonized approaches for reporting cybercrime (i.e.: ransomware attack) incidents and exchange of information. Some of the examples cited to encourage the reporting of cybercrime, and thus contribute to the overall reduction of cyber risks, included the setting of clear guidelines promoting voluntary reporting, building trust, confidentiality, and minimizing the burden on victims and reporting entities.

16. The Chair of the Ad Hoc Committee opened the floor for questions and statements by multi-stakeholders, Member States and non-member observer States. In relation to cross-border access to data from the perspective of Internet service providers, it was clarified that such access would imply a request for user data addressed by one jurisdiction to the Internet service provider located and having possession or custody of such data in other jurisdictions. Complying with the laws of one jurisdiction, which may be conflicting with the laws of another jurisdiction, was identified as the biggest challenge faced by large technology companies. Several speakers reiterated the importance of using technology-neutral language to ensure the future convention remained relevant. While acknowledging that the convention might need to be reviewed or amended at some point in time, several speakers emphasized the importance of an inclusive approach to the negotiations, to consider the views of not only large, but also smaller companies and other stakeholders. States were encouraged to establish formal procedures for requesting and receiving feedback on legislation from the private sector as a way of engaging such sector in the potential future implementation review mechanism of the convention. The potential role of the future convention in harmonizing legislation and hence expediting cybercrime investigations through more efficient public-private partnership cooperation was highlighted. Furthermore, several speakers noted that the convention could articulate the important role of the private sector in investigations of the use of information and communications technologies for criminal purposes, as well as in capacity-building and awareness-raising activities. While highlighting the benefits of involving multi-stakeholders in the provision of capacity-building and technical assistance, several speakers underscored that such assistance should build on existing mechanisms and be carried out on a voluntary basis. The role and commitment of the private sector in upholding human rights standards was also underlined.

17. At its fourth meeting on 4 November 2022, the Third Intersessional Consultation of the Ad Hoc Committee was adjourned after all agenda items were considered.