

23 March 2023

English only

**Ad Hoc Committee to Elaborate a
Comprehensive International Convention
on Countering the Use of Information and
Communications Technologies for
Criminal Purposes**

Fifth session

Vienna, 11–21 April 2023

**Chair's Report of the Fourth 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 Fourth Intersessional Consultation, held on 6 and 7 March 2023.
2. The Fourth 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 Fourth Intersessional Consultation was held in English over four meetings in Vienna and online (the agenda is available [here](#)). It was attended by representatives of 59 multi-stakeholders: 3 from United Nations bodies, specialized agencies, funds and functional commissions of the Economic and Social Council, 7 from intergovernmental organizations, 19 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 61 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 H.E. Mr. Mohamed Hamdy Elmolla (Egypt), Vice-Chair of the Ad Hoc Committee.
5. A panel discussion was held under agenda item 2, entitled “Effective and responsive cooperation and other aspects of the chapter on international cooperation”, with presentations by Ms. Mary Rodriguez, Executive Director of Legal Affairs at INTERPOL, Ms. Youngjin Song, Lecturer at Sung Kyun Kwan University, Mr. Wolfgang Schwabl, Chief Security Officer at A1 Telekom Austria AG, Ms. Tima Soni, Chief Information Security Officer and Chief of the Cybersecurity Division at the United Nations International Computing Centre, and Mr. Nemanja Malisevic, Director of Digital Diplomacy at Microsoft Cooperation.
6. The panellists presented on various aspects of international cooperation in criminal matters. The first panellist addressed matters of mutual legal assistance (MLA) and mentioned that traditional MLA requests faced several challenges, namely, the fact that they entail highly bureaucratic processes among multiple jurisdictions in addition to the lack of resources, in many cases, to support the work of relevant authorities. The panellist further stated that MLA in the context of information and communications technologies for criminal purposes added another element of complexity, particularly when seeking the preservation of communication records held by private companies or when requesting basic subscriber information, traffic- or content data, due to the different evidentiary standards required by the country holding the data. In addition, the panellist stated that there was general agreement among the international community that traditional MLA requests were very slow, and she underscored the unique opportunity presented by the draft convention to address this issue. Furthermore, she highlighted the role her organization could play in supporting Member States in MLA and extradition requests. The second panellist presented on the challenges of law enforcement access to cloud data in the context of criminal investigations. After explaining the complex nature of cloud data, namely the uncertainty of its location and potential dispersion across multiple jurisdictions, the panellist elaborated on the difficulty for law enforcement agencies to efficiently investigate and prosecute cybercrime when dealing with cloud data. Drawing on comparative research, she presented the categorization of law enforcement access to data in direct and indirect data collection and further mentioned data-collection factors to consider in the process of drafting the convention. After mentioning that effective and efficient international cooperation must be based on solid national cooperation among all relevant stakeholders, the third panellist presented the overview of a national case as a best practice for the cooperation between law enforcement authorities and stakeholders in developing a mechanism of cooperation in criminal investigations between relevant authorities and the private sector. In particular, the example addressed the challenges of an effective data retention mechanism that struck a balance between human rights considerations and law enforcement powers to combat cybercrime. The fourth panellist presented challenges and experiences by several United Nations organizations in relation to the use of information and communications technologies for criminal purposes and elaborated on the types of cyber-attacks experienced by the different organizations and potential solutions through their flagship service entitled Common Secure Threat Intelligence, which has a unique and cross-cutting perspective on cyberattacks against United Nations targets. Lastly, the fifth panellist began by stressing the preference for a narrow and well-defined scope of criminalization and cautioned that a broader scope could be counterproductive to the objectives of the future convention by hampering law enforcement agencies in the fight against information and communications technologies for criminal purposes. He further stated that having a clear definition of cybercrime is paramount for service providers to be able to effectively cooperate with authorities. The panellist further presented a range of concrete proposals on the provisions contained in the consolidated negotiating document.

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. Following a question to the third panellist on his presentation of a national case and the resulting national cooperation mechanism between law enforcement and the private sector, in particular whether it could be applicable to other Member States, a panellist specified that the model could be applied to other countries, allowing enough time and the correct identification of participating stakeholders. Nevertheless, the geographical dimension of the Member State interested in implementing that model was mentioned as a potential challenge. Another issue that received considerable attention was the matter of trust between stakeholders and law enforcement agencies with regard to international cooperation and the appropriate means to build it. Several speakers stressed the fact that trust was at the heart of the issue and that it needed to be built over time. In this regard, Member States were cautioned not to reinvent the wheel, but to formulate clear objectives and have the will to meet and cooperate. Moreover, the importance of strong safeguards in the convention was mentioned by some speakers as a practical and effective way to promote trust and thus strengthen the implementation of the future convention. In this context, several speakers stressed the paramount importance of predictability for ascertaining the competent point or points of contact to process MLA requests. Finally, while using language from other relevant international instruments was highlighted as a good practice by some speakers, the dangers of doing so in a selective way without holistically considering the original text was underscored by others.

8. The discussion under agenda item 3, entitled “Technical assistance: setting priorities for the delivery of technical assistance, in particular to developing countries”, was preceded by a panel with presentations by Ms. Martha Stickings, Deputy Head of Strategic Police Matters Unit, Adviser on Cybercrime at the Organization for Security and Co-operation in Europe (OSCE), Ms. Mariya Heletiy, Deputy Chief of Party at the Initiative Centre to Support Social Action “Ednannia”, Ms. Tereza Horejsova, Outreach Manager at the Global Forum on Cyber Expertise (GFCE), Mr. Christian Ohanian, Senior Counsel for Privacy and Cybersecurity for Cyber & Intelligence Solutions at Mastercard on behalf of the International Chamber of Commerce, and Mr. John Ede, President of Ohaha Family Foundation.

9. When specifying the particular importance of technical assistance in the fight against cybercrime, the first panellist mentioned that criminal justice systems had difficulties keeping pace with the challenges posed by the constant developments in technology and presented on different aspects of technical assistance to effectively support law enforcement practitioners. The need of a cross-dimensional and comprehensive approach to technical assistance was highlighted, as was the importance of including a training on cybercrime and electronic evidence in all basic trainings for law enforcement. She further underscored the importance of enhancing public-private partnerships (PPPs) in the context of the provision of technical assistance, especially the cooperation of law enforcement agencies with the private sector across different jurisdictions. Moreover, the panellists highlighted the crucial role of women in developing, delivering and implementing technical assistance and capacity-building, for which a strong gender mainstreaming approach was needed. The second panellist discussed how the use of information and communications technologies for criminal purposes affects civil society and addressed lessons learned from a national case. The third panellist emphasized the central role of the private sector in the provision of effective technical assistance to law enforcement practitioners and further presented some tools provided by her organization to better understand the needs and priorities of Member States, such as working groups to bridge the divide between different stakeholders, or targeted research, to clearly identify gaps in research on cybercrime matters. The fourth panellist mentioned that, while fostering and strengthening international cooperation is one of the main objectives of the draft convention, international cooperation would yield positive results only through successful technical assistance and capacity-building measures and reiterated the central role of public-public

partnerships to fight the use of information and communications technologies for criminal purposes. In discussing the role of the private sector, he noted the need to develop targeted technical assistance programmes as different countries have different needs, the fact that well-balanced relations between private companies and governments was possible, and the importance of appropriate safeguards for human rights and data protection. With regard to the last point, the panellist emphasized that strong human rights safeguards in the draft convention would be a gateway to fostering more robust collaborations with the private sector. In his presentation, the fifth panellist also stressed the role of the private sector in the provision of technical assistance to effectively prevent and combat cybercrime and mentioned the need for a secure and reliable feedback mechanism to the assistance provided. Furthermore, the panellist underscored the overlapping nature of technical assistance and preventive measures, in particular awareness-raising.

10. Following the presentations, the Vice-Chair of the Ad Hoc Committee opened the floor for questions and statements on agenda item 3. Some speakers stressed the importance of mainstreaming a gender perspective in technical assistance approaches, and of moving beyond a perspective that perceives women only as victims of cybercrime but understands them also as key actors in both its perpetration and prevention. The meeting also discussed how stakeholders could help Member States prioritize among the many potential areas for capacity-building efforts, in order to effectively counter the use of information and communications technologies for criminal purposes. In this regard, speakers emphasized the role of the private sector in providing solution-oriented and practical assessments in the design and delivery of technical assistance. In relation to a question on the follow-up to technical training and the experience of monitoring its implementation to ensure its continued effectiveness, speakers stressed the need for a comprehensive approach and transparency in the evaluation of the delivery of technical assistance, particularly through communication between implementing actors to avoid duplication of efforts. Also to avoid duplication of efforts when discussing the effective and efficient provision of technical assistance to countries, the cooperation between regional and international organizations was accorded particular importance by some speakers. In this regard, one panellist provided further insight into the way her organization cooperated with other international organizations, including UNODC, in the delivery of joint trainings or through the use of tools and publications designed by other entities. The panellist further underscored the benefit of sharing training material on criminal justice matters as well as nominating the same individuals for several relevant training exercises to build comprehensive skills set among practitioners and avoid the disaggregation of skills. Moreover, speakers highlighted the importance of preserving an open and ongoing dialogue with the entire range of stakeholders. On the matter of designing technical assistance and capacity-building trainings that adequately considered human rights standards, speakers elaborated on the importance to conduct a needs assessment at the national level to identify the most pressing issues and to mainstream human rights in the entire process of design and delivery of technical assistance.

11. Under agenda item 4, entitled “Striving to remain one step ahead: thinking beyond traditional prevention approaches”, a panel discussion was held with presentations by Mr. Pierre-Jean Clause, President of Generation Maastricht, Mr. Camilo Tamayo Gomez, Senior Lecturer at the University of Huddersfield, Mr. Fotios Spyropoulos, Vice President of the Board of the Centre for the Study of Cybercrime and Mr. Ed Cabrera, Chief Cybersecurity Officer at TrendMicro on behalf of Tech Accord.

12. The first panellist addressed cybercrime prevention from the perspective of children and youth. He stressed the importance of regular assessments of cyberthreats and criminal trends, which should go hand-in-hand with strong privacy and security measures. The panellist also emphasized the importance of educating children and young people, as well as promoting investment in cybersecurity training and relevant personnel with a focus on children and youth. The second

panellist elaborated on the role and importance of citizen-led approaches in the context of preventing cybercrime and stressed the need for Member States to consider civil society in their prevention policies as subjects with agency, that is, as individuals with the capacity to affect change, rather than potential victims without influence. In this context, he gave a wide range of examples and initiatives within grass-roots movements and from-below approaches, ranging from education and community-based reporting to online response systems, civilian-led cooperation with law enforcement and victim support programmes. The third panellist commented on the role of “technoethics” and criminal law in developing preventive measures against the criminal misuse of information and communications technologies. Covering different aspects of the evolving legal and societal changes driven by technological developments, the presentation explored the formation of “technoethics” as the new ethical guidelines of the digital society, which was said to be the most important stakeholder in cybercrime prevention. The panellist emphasized the importance of overcoming the outdated dichotomy between the online and offline worlds as it is no longer representative of today’s reality. Through the presentation of a private sector case, the fourth panellist explained the role that cybersecurity companies can play in crime prevention. Potential contributions from private companies to crime prevention include real-time threat intelligence sharing with consumers as well as international cooperation between relevant stakeholders, law enforcement and governments. The panellist also highlighted the particular importance of PPPs in the design and implementation of successful cybercrime prevention measures.

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. Following a question from the floor, a panellist provided further details of the research supporting his presentation on exploring citizen-led and “from below” approaches to crime prevention when addressing cybercrime, specifying that the results discussed at the meeting were based on research conducted in Europe and Latin America and that research in other areas of the world would follow to complement the conclusions. The importance of understanding how technology is used in different parts of the world was also underscored by the panellist, as different types of technologies closely related to the most prevalent type of crime in each region, thus becoming particularly relevant for the development of different approaches to design and implementation of effective preventive measures. Regarding a comment on the importance of the empowerment of potential victims as a means of prevention, a panellist highlighted the often-underestimated role of solidarity within communities as a central source of empowerment of civil society, especially in communities faced with challenges such as access to education, health or justice. Furthermore, when discussing public-private partnerships in relation to prevention, removing barriers of liability for the private sector was emphasized by another panellist as an important tool for this sector to be able to proactively cooperate with law enforcement authorities in a timely and preventive manner.

14. A panel discussion was also held under agenda item 5, entitled “Laying the foundation for an effective convention: the mechanism of implementation”, with presentations by Mr. Mohammed Masood Mohiuddin, Chairman of the Aim Education & Research Society, Ms. Omoyemen Lucia Odigie-Emmanuel, Director of the Centre for Human Rights and Climate Change Research and Ms. Summer Walker, Head of Multilateral Affairs at the Global Initiative against Transnational Crime (GI-TOC).

15. The first panellist highlighted the many ways in which information and communications technologies could be used for criminal purposes and stressed the importance of keeping up with criminal trends. According to him, any implementation of the future convention should, thus, consider the multidimensional nature of cybercrime. The second panellist outlined several elements that any effective implementation mechanism should consider, in particular the collection of

data to analyse implementation, its design as a peer or expert review process, and participation of stakeholders in the decision-making process. She also stressed the need to anticipate the implementation mechanism when drafting the convention and warned that several international conventions have been frustrated at the national and international levels by a variety of factors. Echoing these warnings, the third panellist stressed that the implementation mechanism should focus on the impact of the treaty on society, which could best be achieved by ensuring the inclusiveness of the mechanism, its expert-led nature, ongoing data and trend analysis, and policy coherence with other existing bodies within the international system, including on human rights. She also underscored that building and maintaining trust between States parties and stakeholders was an important part of implementation.

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. Views were exchanged on the mechanisms of implementation of existing international instruments in the area of crime prevention and criminal justice, namely on the existence of good practices to consider and, alternatively, on lessons learned to be aware of when drafting the chapter on the mechanism of implementation of the future convention. Concerning novel ways to consider a mechanism of implementation for the future convention, one panellist specified that, should a conference of the parties or similar subsidiary body be created, it could look at the impact of legislative developments in line with the convention instead of becoming a forum for the presentation by States parties of legislative developments without an in-depth analysis of its effects. In this regard, one panellist stressed the importance of considering a robust mechanism of implementation from the early negotiating stages of the future convention, given that negotiating new rules, including those that consider the engagement of multi-stakeholders, at a later stage might hinder an effective implementation of the convention. Moreover, considering the complex and border-less nature of cybercrime, and how different intergovernmental bodies in Vienna have addressed different cyber-related issues in their work, one speaker considered the viability of merging the mechanism of implementation of the future convention with mechanisms of implementation of the subsidiary bodies of relevant existing international instruments, such as the United Nations Convention against Transnational Organized Crime (UNTOC), the United Nations Convention against Corruption (UNCAC), the Single Convention on Narcotic Drugs, the Convention on Psychotropic Substances and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. It was mentioned that such an approach would promote coherence and consistency among the different bodies and could contribute to a more efficient use of resources. In addition, the inclusive nature of the work of the Ad Hoc Committee to date was highlighted by a number of speakers as a novel element worth retaining in the development of an implementation mechanism for the future convention.

17. At its fourth meeting on 7 March 2023, the Fourth Intersessional Consultation of the Ad Hoc Committee was adjourned after all agenda items were considered.