United Nations E/CN.15/2022/6

Economic and Social Council

Distr.: General
4 March 2022

Original: English

Commission on Crime Prevention and Criminal Justice
Thirty-first session
Vienna, 16–20 May 2022
Item 5 of the provisional agenda*
Thematic discussion on strengthening the use of digital evidence in criminal justice and countering cybercrime, including the abuse and exploitation of minors in illegal activities with the use of the Internet

Guide for the thematic discussion on strengthening the use of digital evidence in criminal justice and countering cybercrime, including the abuse and exploitation of minors in illegal activities with the use of the Internet

Note by the Secretariat

Summary

The present note has been prepared by the Secretariat as a guide for the thematic discussion of the Commission on Crime Prevention and Criminal Justice at its thirty-first session, pursuant to its decision 18/1. As decided by the Commission at its reconvened thirtieth session, the prominent theme for the thirty-first session will be "Strengthening the use of digital evidence in criminal justice and countering cybercrime, including the abuse and exploitation of minors in illegal activities with the use of the Internet".

The present note provides updated information and describes trends and challenges related to legal, policy and operational aspects. It also outlines possible responses and raises questions and issues that the Commission may wish to discuss.

* E/CN.15/2022/1.

V.22-01255 (E) 170322 180322

I. Introduction

1. At its reconvened thirtieth session, the Commission on Crime Prevention and Criminal Justice decided that the prominent theme for its thirty-first session would be "Strengthening the use of digital evidence in criminal justice and countering cybercrime, including the abuse and exploitation of minors in illegal activities with the use of the Internet". The Secretariat prepared the present note in accordance with decision 18/1, in which the Commission decided that the discussion on the prominent theme would be based on a discussion guide including a list of questions to be addressed by participants.

2. The prominent theme covers various important topics covered by the Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law: Towards the Achievement of the 2030 Agenda for Sustainable Development, adopted by the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice, held in Kyoto, Japan, from 7 to 12 March 2021, with regard to which States declared that they would endeavour to take action. It is therefore hoped that the present note can underpin and enrich the Commission's discussion and support advancements in the effective implementation of the various international standards referred to below, as well as the Kyoto Declaration.

II. Strengthening the use of digital evidence in criminal justice

A. Current situation and challenges

Procedural investigative powers

3. Crime involving electronic evidence [1] presents unique challenges for the authorities entrusted with responding to it. An examination of the legal basis for investigative powers used in crimes involving electronic evidence reveals considerable diversity in approaches at the national level in terms of discrepancies in evidentiary rules and the conditions, safeguards and investigative powers for the collection and use of electronic evidence in criminal justice matters, as prescribed in national criminal procedure codes or other specific laws. An important consequence of such diverse approaches has been the emergence of legal fragmentation [2] on an increasing scale, which, in turn, may create inconsistencies in the exercise of procedural powers and hamper investigation efforts. [3]

4. The most common types of investigative measures for gathering electronic evidence include the expedited preservation and disclosure of stored computer data; the production of stored computer data (including in emergency situations); search and seizure; electronic surveillance; and interception of content data.

5. While important law reform efforts are taking place domestically in many Member States (with the introduction of provisions on access to, control of and

[1] In many contexts, the terms "electronic evidence" and "digital evidence" are used interchangeably. In the present document, the term "electronic evidence" is used, following its use in similar contexts (e.g. thematic discussion of the Commission at its twenty-seventh session) and regional initiatives (see the Guidelines on electronic evidence in civil and administrative proceedings adopted on 30 January 2019 by the Committee of Ministers of the Council of Europe), unless otherwise provided (references to the title of the thematic discussion at the thirty-first session of the Commission, as well as references in some footnotes).

[2] Counter-Terrorism Committee Executive Directorate, "The state of international cooperation for lawful access to digital evidence: research perspectives", CTED Trends Report, January 2022, pp. 23–24.

[3] United Nations Office on Drugs and Crime (UNODC), *Digest of Cyber Organized Crime* (Vienna, 2021), p. 109.

sharing of data),[4] a significant number are yet to adapt their legal frameworks to the sophistication and digital nature of contemporary forms of crime.

6. In parallel, important initiatives have been undertaken at the international level, each of them in different stages of development, with a view to formulating international standards to regulate issues relating to lawful access to, as well as use and sharing of, electronic evidence. The Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which is representative of all regions, was established in accordance with General Assembly resolution 74/247. At the regional level, relevant initiatives include the adoption, in November 2021, of the Second Additional Protocol to the Council of Europe Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (to be opened for signature in May 2022) and the elaboration of a draft regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. These instruments are aimed at resolving key aspects of the problems associated with (cross-border) access to electronic evidence for law enforcement and judicial purposes.

Cross-border cooperation with communications service providers

7. Securing electronic evidence located in another jurisdiction or on cloud-based servers poses challenges owing to the volatile nature of such evidence. International cooperation requires a timely response, including the preservation and production of data by communications service providers, and the ability to request specialized investigative action. One challenge commonly encountered when requesting such data from another jurisdiction is delays in the response that often exceed the data-retention period and may enable perpetrators to permanently destroy key electronic evidence.[5] For that reason, it is extremely important to forge partnerships between online communication service providers and law enforcement agencies.

8. The role of communication service providers in criminal justice and international cooperation in criminal matters remains a critical yet not entirely explored topic. Communication service providers are the private entities in possession of users' electronic data and, as such, the recipients of an increased volume of requests from law enforcement authorities seeking to preserve and/or access electronic data of probative value for a criminal investigation. Depending on their location, communication service providers may be subject to telecommunications and industry-specific regulations.

9. An increased number of communication service providers have issued guidelines for law enforcement and judicial authorities that are aimed at clarifying the requirements and processes for the submission of requests involving electronic evidence, including on what types of evidence could be requested, the preservation of electronic evidence, emergency disclosure and direct requests for voluntary disclosure and data retention. The worldwide dissemination of such guidelines across the law enforcement and judicial community remains a challenge for communication service providers, while the volume of requests from authorities for the disclosure of data has increased. For law enforcement authorities, individual tailored procedures (while helpful) result in the dual challenge of having to reassess their own investigative methods and practices and examining different sources of information, which implies additional time for the preparation of requests and for the investigation itself.[6]

[4] Counter-Terrorism Committee Executive Directorate, "The state of international cooperation for lawful access to digital evidence".

[5] Background paper prepared by the Secretariat on gathering and sharing electronic evidence (CTOC/COP/WG.3/2015/2), para. 19.

[6] European Union Agency for Law Enforcement Cooperation (Europol), *SIRIUS EU Digital Evidence Situation Report: 3rd Annual Report* (2021), pp. 49–50.

10. The capacity of law enforcement and judicial authorities to cooperate with foreign-based communication service providers in accordance with applicable laws and their requirements remains the main challenge, especially in cross-border investigations, where different legal frameworks may overlap or offer different approaches.

Admissibility of electronic evidence in court

11. Scholars suggest that admissibility of evidence in digital form has largely been accomplished through the redefinition of legal concepts in the malleable rules of evidence.[7] General rules of evidence are often applied to the admissibility of electronic evidence in court, in particular in countries where such evidence is neither regulated nor specified in the law. Data from a report surveying countries across the European Union concluded that in the vast majority of the surveyed countries (82.4 per cent), data gathered by authorities through a request for voluntary disclosure to a foreign-based private entity could be admitted as evidence in court.[8] While countries have different legal frameworks, it appears that the lack of legal regulation of this particular power does not prevent authorities sending voluntary disclosure requests to communication service providers, applying domestic general rules of evidence.

12. Along these lines, it is broadly recognized that a neutral approach to technology must prevail in the handling of electronic evidence by courts. Courts should neither discriminate against electronic evidence nor privilege it over other types of evidence, and should be guided by the principle of equality between the parties in relevant proceedings.[9]

13. Despite the emergence of these principles, there seems to be no uniform practice when it comes to the admissibility of electronic evidence in court, in particular if it is collected from foreign-based communication service providers. While some jurisdictions deem certain categories of data (such as basic subscriber information) admissible, under certain conditions (when gathered directly from foreign-based communication service providers through voluntary cooperation), others require a formal judicial request to use the obtained electronic evidence in court in a criminal proceeding (otherwise, it may only be used for intelligence purposes).[10]

14. Admissibility questions should be clarified among all the involved actors at an early stage and, when necessary and possible, with the involvement of the competent courts, which may have an active role in managing evidence. In cross-border investigations, emphasis should be placed on preventing infringements of the admissibility requirements (i.e. chain of custody from seizure to preservation) in force in the requesting State.

Jurisdictional issues

15. Jurisdictional issues are of paramount importance to the use of electronic evidence in criminal justice, as most investigations in which electronic evidence is relevant require a request to a communication service provider based in another jurisdiction. Likewise, data in the cloud are in permanent “migration”, as different parts may be located in different jurisdictions at the same time, leading to difficulties in asserting jurisdiction and knowing where to send requests for electronic evidence.[11]

[7] Stephen Mason and Daniel Seng, eds., *Electronic Evidence*, 4th ed. (London, University of London, Institute of Advanced Legal Studies, School of Advanced Study, 2017), p. 81.

[8] Europol, *SIRIUS EU Digital Evidence Situation Report: 2nd Annual Report* (2020), p. 17.

[9] Committee of Ministers of the Council of Europe, *Electronic Evidence in Civil and Administrative Proceedings: Guidelines and Explanatory Memorandum* (Strasbourg, France, 2019), p. 7.

[10] Europol, *SIRIUS EU Digital Evidence Situation Report: 3rd Annual Report*, p. 50.

[11] UNODC, Counter-Terrorism Committee Executive Directorate and International Association of Prosecutors, *Practical Guide for Requesting Electronic Evidence across Borders* (Vienna, 2019), p. 78.

16. Recent law reform efforts have addressed the challenge of lawful access to electronic evidence in the possession, custody or control of a foreign-based communication service provider by extending jurisdiction. For instance, in 2018, legislation was adopted in the United States of America (Clarifying Lawful Overseas Use of Data Act (CLOUD) Act) that may compel United States communication service providers to share data regardless of whether such data are or were stored in the United States or abroad.[12]

Operational and investigative issues, including international cooperation

17. While the number of requests for mutual legal assistance to obtain and preserve extraterritorial electronic evidence is growing fast, the traditional and often lengthy modalities of cooperation on which Member States still often rely do not facilitate rapid access to key electronic evidence, which is, by its nature, volatile.

18. Efforts to adapt and expedite existing mutual legal assistance processes and frameworks are taking place worldwide. An example is the recently adopted Second Additional Protocol to the Council of Europe Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence. Article 8 of that Protocol requires each State party to adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another party for the purpose of compelling a communication service provider in the requested party's territory to produce specified and stored subscriber information (within 20 days) and traffic data (within 45 days) in that communication service provider's possession or control which is needed for the party's specific criminal investigations or proceedings. In this way, the Protocol establishes a mechanism that complements the mutual assistance provisions of the Council of Europe Convention on Cybercrime. It is designed to be more streamlined than current mutual assistance processes, in that the information that the requesting party must provide is more limited and the process for obtaining the data more rapid.[13] Other features include means for urgent cooperation in emergency situations in which lives are at risk, more effective law enforcement and judicial cooperation to obtain traffic data, and tools for joint investigations.

19. The Treaty on the Electronic Transmission of Requests for International Legal Cooperation among Central Authorities is another regional instrument that will contribute to expediting mutual legal assistance processes, enabling a more rapid cross-border transfer of electronic evidence.[14]

20. Special investigative techniques, including electronic surveillance, undercover operations and controlled delivery, enable law enforcement agencies to gather information in the context of investigations of serious crimes without alerting the target persons. Such special investigative techniques may also include techniques to gather electronic evidence. New technological developments such as anonymization software, high-grade encryption and virtual currencies are encountered when investigating offences involving electronic evidence, and investigators may need to adopt new strategies and consider how to use special investigative techniques and remote digital forensics to gather such electronic evidence while ensuring the admissibility and use of such evidence in court.

21. Differences among countries in criminal procedure laws and the rules of evidence regulating special investigative techniques may hamper cooperation in investigations involving those techniques.[15] A crucial element, however, is compliance with the principle of proportionality when using special investigative

[12] Counter-Terrorism Committee Executive Directorate, "The state of international cooperation for lawful access to digital evidence", pp. 17–19.

[13] See Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence.

[14] Report on the meeting of the Working Group on International Cooperation held in Vienna on 7 and 8 July 2020 (CTOC/COP/WG.3/2020/4), para. 67.

[15] UNODC, *Digest of Cyber Organized Crime Cases*, p. 101.

techniques in cybercrime investigations, especially on the darknet, or when electronic evidence has become relevant to investigations of "conventional" crime. In many domestic legal systems, that principle is tested primarily by the judicial authority supervising the investigation and by the court, as appropriate.[16]

Human rights safeguards

22. The conditions and safeguards for the collection and use of electronic evidence predominantly require judicial or other independent oversight to delineate limits on the procedures, processes, methods and tools used to collect, acquire, preserve and analyse electronic evidence.[17]

23. To avoid the use of special investigative techniques for the gathering of electronic evidence as a "Trojan horse" for potential infringements in the sphere of fundamental human rights, such as the right to privacy and the right to freedom of opinion and expression, special investigative techniques to gather electronic evidence need to be continuously monitored and evaluated in terms of their impact.[18] Another pressing need is to enhance training for law enforcement and criminal justice personnel to make effective and human rights-compliant use of the modern technologies at their disposal.

24. From its inception, the Global Initiative on Handling Electronic Evidence (see paras. 25–26 below) has sought to foster a balance between the handling of electronic evidence for law enforcement and judicial purposes and respect for and protection of human rights. In this regard, it raises the awareness of law enforcement and judicial officials about human rights and related case law. Officials trained under the Global Initiative learn about human rights safeguards such as institutional safeguards, independent oversight mechanisms in the authorization of data-collection and data-sharing measures, effective safeguards for the right of defence, procedural safeguards to notify victims whose right to privacy has been infringed through State-authorized surveillance activities and safeguards against unwarranted and excessive interference in the right to privacy.

Technical and legislative assistance

25. The Global Initiative on Handling Electronic Evidence was launched by UNODC, together with Counter-Terrorism Committee Executive Directorate and the International Association of Prosecutors, in 2017. It focuses on strengthening the capacity of national institutions and officials to combat crimes committed through the use of information and communications technology, as well as those involving electronic evidence.

26. Under the Global Initiative, UNODC commissioned the development of the *Practical Guide for Requesting Electronic Evidence Across Borders*, the data disclosure framework and related practical tools and resources, all available on the electronic evidence hub of the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.[19] Through the Initiative, UNODC is leading the enhancement of public-private partnerships with Member States, international and, regional organizations (such as the European Union Agency for Criminal Justice Cooperation (Eurojust), the European Union Agency for Law

[16] Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019 (UNODC/CCPCJ/EG.4/2019/2), para. 37; and background paper prepared by the Secretariat on international cooperation involving special investigative techniques (CTOC/COP/WG.3/2020/3), paras. 34–35.

[17] UNODC, *Digest of Cyber Organized Crime Cases*, p. 109.

[18] See also the background paper prepared by the Secretariat for workshop 4 (Current crime trends, recent developments and emerging solutions, in particular new technologies as means for and tools against crime) of the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice, (A/CONF.234/11), para. 78.

[19] https://sherloc.unodc.org/cld/en/st/evidence/electronic-evidence-hub.html.

Enforcement Cooperation (Europol) and the European Judicial Network), as well as communication service providers.

Special considerations on child protection

27. When handling electronic evidence in judicial proceedings involving children, special measures need to be put in place to protect children's rights to privacy, safety, well-being and access to justice. These rights are particularly relevant in setting limits to the exercise of investigative powers and enabling procedural safeguards against unnecessary and disproportionate digital interference with privacy. Criminal justice officials must be guided by the principle of the best interests of the child and must handle electronic evidence in such a way that it reduces the burden on child victims as the only source of evidence.

28. Children who are victims of or witnesses to abuse and exploitation committed through the use of the Internet should have access to support services, legal aid and protection measures to prevent revictimization, retraumatization, stigmatization or intimidation. Investigative powers for the collection of electronic evidence in cases involving child victims of abuse and exploitation should be revised to ensure that they do not exacerbate or increase the vulnerabilities of child victims and witnesses.[20]

29. For the collection and use of any type of electronic evidence, including the receipt of evidence on children, it is crucial to protect any information relating to a child's identity and to uphold children's right to privacy at all stages of the proceedings. This entails that information relating to a child's involvement in the justice process be secured (throughout the entire chain of custody process) and that measures should be taken to protect children from undue exposure to the public at all stages of the proceedings.[21]

30. A variety of measures can be taken to assist in the giving of evidence by and the receipt of evidence, including electronic evidence, from children. Such measures concern, for instance, the admissibility of evidence, such as videotaped recordings of statements and the application of closed hearings or procedures, which may include the use of facilities allowing the child to give evidence, without having to see the accused, from a special interview room by means of closed-circuit television.[22] Mechanisms, procedures and guidelines to foster the cooperation of communication service providers (including foreign-based) in investigations and criminal proceedings involving child victims of abuse and exploitation are also necessary.

B. Possible responses

31. UNODC can, through its Global Initiative on Handling Electronic Evidence, continue to build capacity for: (a) law enforcement officials to identify, collect, acquire and preserve the electronic data needed to investigate crimes; (b) prosecutorial and judicial authorities to use those data as evidence in court; and (c) central and competent authorities to handle and exchange those data across borders and jurisdictions, without jeopardizing their admissibility and probative value at court.

32. In the context of public-private partnerships, UNDOC can deliver capacity-building, including on the admissibility of electronic evidence obtained from foreign-based communication service providers, aimed at increasing the knowledge, expertise and skills of criminal justice authorities.

33. In accordance with Conference of the Parties to the United Nations Convention against Transnational Organized Crime resolution 10/4, the Secretariat organized two informal expert group meetings for the revision of the model law on mutual assistance

[20] Convention on the Rights of the Child, arts. 16 and 40, para. 2 (b) (vii).

[21] Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, section X.

[22] UNODC, *Justice in Matters involving Child Victims and Witnesses of Crime: Model Law and Related Commentary* (Vienna, 2009), part two, chap. III, sect. C, art. 28, para. 3.

in criminal matters to include provisions on the gathering of electronic evidence and the use of special investigative techniques. The model guidance, as revised, is brought to the attention of the Commission for the information of Member States and also as a tool, together with available model mutual legal assistance request checklists, for countries seeking support in updating their legislation and streamlining their mutual legal assistance processes relating to electronic evidence.

C. Questions for consideration

34. The Commission may wish to consider the following points for further discussion:

(a) What challenges are encountered by competent authorities when using special investigative techniques to gather electronic evidence in the context of criminal investigations, and what are good practices in response? How can human rights safeguards best be taken into account in this regard?

(b) What experience has been accumulated with the admissibility of electronic evidence in court? What are the lessons learned from the application of general principles of domestic procedural laws and ad hoc evidentiary rules, as well as the development of national jurisprudence, in this regard?

(c) What are the lessons learned from efforts to foster cooperation between law enforcement authorities and communication service providers to secure electronic evidence for the detection, investigation and prosecution of serious crimes and what could be the impact and potential of new initiatives in this field?

(d) How can synergies and partnerships be best pursued among international organizations delivering technical assistance in matters of electronic evidence to provide Member States with tangible and sustainable capacity-building services?

III. Countering cybercrime

A. Current situation and challenges

35. In 2018, the prominent theme for the twenty-seventh session of the Commission was “Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels”. For the thematic discussion, the Secretariat prepared a comprehensive discussion guide examining different aspects of policies and strategies against cybercrime, ranging from criminalization and procedural powers to inter-agency coordination, international cooperation and prevention.[23]

36. Moreover, the Secretary-General, in his report on countering the use of information and communications technologies for criminal purposes, prepared pursuant to General Assembly resolution 73/187, set out the views of 61 Member States on the challenges that they faced in countering the use of information and communications technologies for criminal purposes.[24]

37. The Commission was also informed at its twenty-ninth and thirtieth sessions about the progress made in 2019 and 2020 by UNODC in promoting and delivering cybercrime technical assistance and capacity-building.[25]

38. Building on the above, the present discussion guide is intended to provide a focused update on some recent developments in the field of cybercrime, including the impact of the coronavirus disease (COVID-19) pandemic.

[23] E/CN.15/2018/6.
[24] A/74/130.
[25] E/CN.15/2020/12 and E/CN.15/2021/13.

Policy developments and intergovernmental processes

39. In its resolution 74/247, the General Assembly established the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, established by the Assembly in its resolution 65/230, which held seven sessions, from 2011 to 2021, including a stocktaking meeting.[26]

40. Following the organizational session of the Ad Hoc Committee held in May 2021, the General Assembly, in its resolution 75/282, decided upon, inter alia, the decision-making methods of the Committee and matters relating to participation, and decided to convene at least six sessions of 10 days each and a concluding session, in order to provide a draft convention to the Assembly at its seventy-eighth session. Owing to the impact of the COVID-19 pandemic, the first negotiating session of the Ad Hoc Committee, originally scheduled for January 2022, was postponed by the Assembly by means of its decision 76/552. Accordingly, the Ad Hoc Committee held a session on organizational matters on 24 February and held its first session from 28 February to 11 March 2022.

41. At its first session, the Ad Hoc Committee discussed its mode of work at future sessions and during the intersessional periods and the objectives, scope and structure of the convention, and started a preliminary exchange of views on key elements of the convention.

Prevention

42. Cybercrime presents particular crime prevention challenges. These include the increasing ubiquity and affordability of online devices, leading to large numbers of potential victims; the comparative willingness of persons to assume “risky” online behaviour; the possibility for anonymity and obfuscation techniques on the part of perpetrators; the transnational nature of many cybercrime acts; and the fast pace of criminal innovation. Each of these challenges has implications for the organization, methods and approaches adopted for cybercrime prevention.

43. Cybercrime prevention has become an important component of national policies and strategies to prevent and counter cyberattacks and threats. That was noted during the sixth meeting of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, which was focused, inter alia, on prevention.[27]

44. In particular, collaboration with communication service providers can play a crucial role in cybercrime prevention. Their involvement can range from the active filtering of Internet communications and content with a view to preventing cybercrime acts before they are committed or disrupting them at an early stage to storing user data that law enforcement officials in possession of a warrant can access for use in cybercrime investigations. With regard to the later, the deterrent effect shows how preventive and reactive measures can complement and reinforce each other. The cooperation of communication service providers with national authorities should be based on the rule of law and the protection of human rights.

Capacity-building and technical assistance

45. Continuous efforts are needed to build the capacity of law enforcement and criminal justice actors to respond to rapidly evolving forms of cybercrime. The specialization of national law enforcement agencies has become increasingly common

[26] See UNODC/CCPCJ/EG.4/2021/2.
[27] UNODC/CCPCJ/EG.4/2020/2, para. 50.

and plays a crucial role in facilitating the processes of gathering, analysing and sharing electronic evidence. This specialization is linked primarily to the particular nature of cybercrime, which presents specific challenges related to the definitions of offences, the applicability of laws and evidence-gathering and analysis. The technical skills and capacity of law enforcement agencies will therefore have a direct impact on the effectiveness of a crime prevention and criminal justice response to cybercrime.[28]

B. Possible responses

Prevention

46. Multi-stakeholder cybercrime strategies, which leverage the roles of different actors in the public and private sectors, as well as civil society, are a vital preventive element to address the diverse challenges posed by cybercrime. It is necessary to promote and increase the participation of all relevant actors in the prevention of cybercrime and, in this regard, regional organizations, the private sector and academia could provide key support, in particular to developing countries, to achieve a global culture of cybersecurity.[29]

47. Public-private partnerships, based on mutual trust and confidence in response to the multifaceted challenges encountered in the fight against cybercrime, are useful not only for the raising of awareness, but also for the prevention of cybercrime itself. For example, artificial intelligence tools could be used to detect child sexual abuse and exploitation material distributed online. Public-private partnerships provide the reporting and information-delivery mechanisms needed to investigate and identify perpetrators. Moreover, as reported at the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, the responsibilities of communication service providers need to be clearly defined to ensure that security precautions are undertaken as preventive measures.[30]

48. Effective measures at both the national and the international levels to facilitate the prosecution and punishment of offenders and efforts to prevent further crime by identifying and disrupting ongoing illicit online activities are considered, in the light of their deterrent effect, a significant component of preventive policies against cybercrime. Of relevance in this regard is also the necessity of investing in capacity-building to upgrade the skills of officers from the whole spectrum of the criminal justice system, who should be involved at the national level in the prevention and investigation of cybercrime.

49. Building upon different investigation techniques and technologies that have been developed to detect cybercrime, it remains essential to continue developing insights into the behaviour of the contemporary cybercriminal utilizing intelligence analysis, criminological research and profiling techniques to deploy existing resources more effectively and to proactively identify features of future communications technologies vulnerable to criminal exploitation.

Capacity-building and technical assistance

50. The Global Programme on Cybercrime assists Member States in combating cybercrime in four main areas: (a) capacity-building; (b) prevention; (c) cooperation; and (d) legal frameworks.

51. Specific techniques and technology, such as artificial intelligence, have become essential in cybercrime investigations. However, their use requires prior analysis of the legality, necessity and proportionality of the measures and technology chosen, and the least restrictive method in terms of the rights to be protected should be considered.

[28] CTOC/COP/WG.3/2015/2, para. 14.
[29] UNODC/CCPCJ/EG.4/2020/2, para. 53.
[30] Ibid., para. 54.

52. Member States continue to strengthen their capacities in countering cybercrime through the establishment of specialized forensic laboratories, police units and prosecutor's offices. UNODC has assisted Member States in this regard by providing training, mentoring and equipment and designing guidelines and standard operating procedures.

C. Questions for consideration

53. The Commission may wish to discuss the following questions:

(a) What are the lessons learned, good practices and challenges encountered in implementing preventive strategies against cybercrime? How can the outcome of such strategies be best monitored, evaluated and measured?

(b) How can academic institutions, the private sector and non-governmental organizations, as well as intergovernmental organizations, best contribute to the development and sharing of knowledge, legislation and policy in the area of cybercrime? How can they collaborate with Member States in the detection and investigation of cybercrime?

(c) What is the accumulated experience of Member States regarding balancing the protection of human rights such as the right to privacy (data protection) and freedom of opinion and expression, on the one hand, and the effectiveness of criminal justice and law enforcement responses to cybercrime, on the other?

(d) Which aspects of cybercrime-related measures have high priority for technical assistance and capacity-building, in particular in view of the evolving nature of cybercrime and the increased use of technology owing to the COVID-19 pandemic?

IV. Abuse and exploitation of children in illegal activities with the use of the Internet

A. Current situation and challenges

54. It is assumed that two thirds of the world's population now have access to the Internet. Among those connected, 60 per cent live in developing countries and 45 per cent are aged 25 or younger. The expanding number of Internet users has resulted in a global rise in the number of potential cybercrime victims and cybercriminals, as predicted by UNODC at the beginning of the pandemic.[31] In this context, gender and age are vulnerability factors. Children, in particular girls, are more likely to become victims of cybercrime, especially online harassment, sexual abuse and trafficking for different types of exploitation with the use of information and communications technologies.

Child online sexual abuse and exploitation

55. Online child sexual abuse and exploitation include the production of child sexual abuse material, but also "cyberenticement", "solicitation" and "online grooming", which are terms commonly used collectively or interchangeably to describe communications made by adults through the use of information and communications technology for the purpose of sexually abusing or exploiting children.[32] The effects of information and communications technology on common existing forms of child sexual abuse and exploitation include enhanced access to victims and child sexual abuse material, increased profits for criminal enterprises, a reduction in the offenders' risk of detention and provision of social affirmation for

[31] UNODC, "Cybercrime and COVID-19: risks and responses" (April 2020).

[32] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienna, 2015), p. 11.

offenders.[33] Of particular concern are new forms such as made-to-order child sexual abuse material, user- and self-generated content, including "sexting", and the livestreaming of child sexual abuse and exploitation.[34]

56. In 2021, independent surveys confirmed that the scale and complexity of online child sexual abuse and exploitation are increasing and that children today face a sustained threat in that regard.[35] Reports by Europol also confirm that activity around the distribution of child sexual exploitation material online appears to be on the increase, on the basis of a number of indicators. The COVID-19 pandemic and related restrictive measures seem to have accelerated this trend[36] and children may be more inclined towards the self-production of content for exchange with peers or adults. The Internet Watch Foundation received 68,000 reports of self-generated child sexual content in 2020, representing a 77 per cent increase over 2019.[37]

Trafficking in children by means of the Internet and other forms of online abuse and exploitation

57. Information and communications technology is increasingly used by perpetrators of trafficking in persons[38] for everything from identifying future victims to exploiting them. Personal information is often made available online by children, especially on social media platforms and gaming sites, enabling targeted profiling for the grooming of victims, while preserving the anonymity of perpetrators. Traffickers have taken advantage of new technologies to refine their methods of control over victims, for example through threats and deception by means of which criminals come to possess intimate material related to their victims, which they then use to blackmail them.[39]

58. Trafficking for sexual exploitation constitutes the majority of detected cases of trafficking for exploitation online and a large share of the victims are children. In recent years, the number of reports of online child sexual abuse material has grown exponentially.

59. Information and communications technology enlarges the pool of children who may be sexually exploited by traffickers and the number of their potential clients, owing to a lack of physical and geographical limitations.[40] In addition, such technology has enabled traffickers to maximize profits through large economies of scale, for example by commercializing and exploiting children through live-streaming on multiple websites, allowing the videos to be watched limitlessly, and selling their services to many clients through the same advertisement on numerous platforms. Organizations such as the National Center for Missing and Exploited Children of the United States and the International Criminal Police Organization (INTERPOL) have

[33] Ibid., pp. 15–20.

[34] Ibid., pp. 21–22; and Chloe Setter and others, *Global Threat Assessment 2021* (WeProtect Global Alliance, 2021), p. 54.

[35] Setter and others, *Global Threat Assessment 2021*.

[36] United Nations Sustainable Development Group, "Policy brief: the impact of COVID-19 on children" (April 2020), p. 3; and Europol, "Catching the virus: cybercrime, disinformation and the COVID-19 pandemic" (April 2020), p. 9.

[37] Setter and others, *Global Threat Assessment 2021*.

[38] In article 3 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, trafficking in persons is defined as "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation."

[39] Background paper prepared by the Secretariat on successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons (CTOC/COP/WG.4/2021/2), para. 18.

[40] UNODC, *Global Report on Trafficking in Persons 2020* (United Nations publication, 2021), p. 122.

reported a large increase in the number of cases of online child trafficking and child sexual exploitation since the beginning of the pandemic.[41]

60. Online child trafficking occurs on the clearnet and on darknets, which are also used to archive and conceal materials and enable perpetrators to better hide illegal material from investigators.

Recruitment and exploitation of children by organized criminal and armed groups, including those designated as terrorist groups, with the use of the Internet

61. The recruitment and exploitation of children by organized criminal and armed groups, including those designated as terrorist groups, is a serious form of violence against children, prohibited by international law. States are required to criminalize it and to take all appropriate measures,[42] ensuring that, when in contact with national authorities, these children are considered and treated primarily as victims.[43]

62. The use of information and communications technology and its role in the recruitment and exploitation of children by such groups is a relatively new means of disseminating propaganda and expands the reach of the groups' messages.[44] Children are at particular risk owing to their ongoing physical and psychological development and because they are active Internet users. Social media platforms, email, chat rooms, e-groups and video recordings are especially popular recruitment tools that can facilitate the grooming of victims. In addition, "targeted advertising" can also be used to identify vulnerable groups such as children to tailor the narrative to suit the audience.[45]

63. Organized criminal and armed groups, including those designated as terrorist groups, may take advantage of children's vulnerability to potentially recruit and exploit them, in particular when this vulnerability is exacerbated, as it has been during the COVID-19 pandemic. This crisis has amplified misinformation on social media and created new opportunities for these groups, including the exploitation of vulnerabilities in the social media ecosystem to manipulate individuals and disseminate conspiracy theories.[46] Online recruitment strategies by such groups have focused on the dissemination of alternative and counter-narratives, which is why mechanisms need to be put in place so that individuals seeking terrorist and violent extremist content are redirected towards media providing messages countering the propaganda of such groups.[47]

Challenges for child victims of online abuse and exploitation

64. The use of the Internet with the purpose of abuse and exploitation of children has served to increase levels of harm suffered by victims, as technologies such as peer-to-peer file-sharing have exacerbated the distribution of child sexual abuse material and cloud-computing technology has enabled private access to storage that

[41] Patricia Davis, "100,000,000: the race to save children behind the staggering number", National Center for Missing and Exploited Children, 1 December 2021.

[42] General Assembly resolution 69/172.

[43] Security Council resolution 2427 (2018); and principles relating to the status of national institutions for the promotion and protection of human rights (the Paris Principles). See also UNODC, "Roadmap on the treatment of children associated with terrorist and violent extremist groups" (Vienna, 2019).

[44] Security Council resolution 2331 (2016) on the misuse of information and communications technology to facilitate trafficking in persons by terrorist groups.

[45] UNODC, *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice Section* (Vienna, 2017), p. 13.

[46] United Nations Interregional Crime and Justice Research Institute, "Stop the virus of disinformation: the risk of malicious use of social media during COVID-19 and the technology options to fight it" (Turin, Italy, 2020), p. iii.

[47] UNODC, *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups*, p. 33.

can host extensive amounts of material at a low cost.[48] In addition, online abuse is often underreported, and challenges for children to report and access justice have been exacerbated by the COVID-19 pandemic, as restrictions on movement have reduced children's access to support persons such as teachers to report incidents at home or online, while social work and related legal and protective services for children may have been suspended or scaled back owing to social-distancing measures.[49]

65. Victimization risk factors for child victims of online abuse and exploitation include gender and sexual orientation, prior abuse and family dysfunction, poverty and migration, age, risky online behaviour and inattention to online safety and privacy, as well as social isolation.[50] The pandemic has increased those risks, as described above.

66. When accessing the justice system and reporting incidents of crime and violence, child victims of crime and violence traditionally face numerous challenges, with their rights often not being adequately recognized. It is crucial to recognize that children, and more specifically child victims, are vulnerable and require special protection as a result of their age, level of maturity and individual needs.[51] Acknowledgment of the victim status of child victims of online abuse and exploitation is a precondition for them having access to rights as victims of crime, especially as participants in legal proceedings and concerning their rights to reparation and rehabilitation. Child victims who do not receive proper child- and gender-sensitive consideration and protection may be revictimized during their contact with the justice system, which can leave them more vulnerable to future violence and reduce the likelihood of them reporting violent crime.[52]

Challenges faced by Member States in preventing and responding to online child abuse and exploitation

67. Cybercrime, including online child abuse and exploitation, is an extremely complex crime to handle. It takes place in the borderless realm of cyberspace and victims, offenders and the tools used can be, and often are, in different countries. Offences occur on both regulated and unregulated platforms (clearnet and darknets), which may hinder the collection of reliable data and statistics.[53] The majority of evidence in cybercrime offences is electronic and frequently requires the use of special investigative techniques, as well as formal and informal international cooperation.

68. The criminalization of cybercrime acts is still insufficient in many countries, as is the effective detection, investigation and prosecution of online child abuse and exploitation, including the generation of clear evidence trails through the use of image analysis and image databases, digital forensics, automated search, data mining and analytics, and undercover operations. When it comes to the prosecution of these crimes, improved mechanisms for international cooperation are crucial as many Member States may still rely on traditional cooperation mechanisms for obtaining extraterritorial evidence in these cases.

69. Finally, Member States may face challenges, such as a lack of coordination mechanisms, in effectively protecting children from this serious form of violence. Tackling those challenges is key in order to ensure a response to the phenomenon that promotes a whole-of-society approach and enhances public-private partnerships and

[48] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, p. 19.

[49] United Nations Sustainable Development Group, "Policy brief: the impact of COVID-19 on children", p. 10.

[50] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, pp. 23–27.

[51] Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, para. 7.

[52] United Nations Model Strategies and Practical Measures on the Elimination of Violence against Children in the Field of Crime Prevention and Criminal Justice.

[53] Europol, *IOCTA 2016: Internet Organised Crime Threat Assessment* (The Hague, 2016).

coordination and cooperation among various institutions and actors (e.g. the justice, child protection, education, health and security sectors).

Examples of evidence-based and evaluated initiatives aimed at overcoming some of the challenges

70. The We Protect Global Alliance is a global network that has the objective of ending online child sexual exploitation and abuse. Its members include 98 Governments, 52 companies, 64 civil society organizations and nine international organizations. It publishes documentation such as the *Global Threat Assessment 2021* and the "Guidance note on implementing the global strategic response to eliminate child sexual exploitation and abuse online".

71. The Working Group on Trafficking in Persons has highlighted innovations in technological investigative tools, such as PhotoDNA and databases that improve forensic processes for investigations into the trafficking of children and child sexual abuse.[54]

Policy developments and international frameworks

72. The Convention on the Rights of the Child outlines minimum standards of protection to which children are entitled, including protection from harmful influences, abuse and exploitation. The Optional Protocol on the sale of children, child prostitution and child pornography is focused exclusively on addressing child sexual abuse and exploitation. The United Nations Convention against Transnational Organized Crime provides for a range of provisions concerning international cooperation against transnational organized crime and its Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, requires States parties to criminalize trafficking in persons, including children.

73. Recognizing the pressing need to address the issue of violence against children and, in particular, the role of the criminal justice system, in 2014, the General Assembly adopted the United Nations Model Strategies and Practical Measures on the Elimination of Violence against Children in the Field of Crime Prevention and Criminal Justice. Furthermore, the Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, adopted in 2005 by the Economic and Social Council, set forth good practices based on the consensus of contemporary knowledge and relevant international and regional norms, standards and principles.

74. In its resolution 74/174, on countering child sexual exploitation and sexual abuse online, the General Assembly urged Member States to criminalize such crimes and to strengthen their efforts to combat cybercrime in relation to child sexual exploitation and sexual abuse, including when committed online.

75. In the 2021 Political Declaration on the Implementation of the United Nations Global Plan of Action to Combat Trafficking in Persons, Member States noted with concern the increasing misuse of information and communications technology to facilitate various aspects of trafficking in persons and various forms of exploitation, including online child sexual exploitation, and emphasized the importance of countering such misuse while respecting human rights.

76. Relevant regional instruments include the Council of Europe Convention on Cybercrime, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the Association of Southeast Asian Nations Convention against Trafficking in Persons, especially Women and Children, the Inter-American Convention on International Traffic in Minors and the African Charter on the Rights and Welfare of the Child.

77. Most recently, the European Union adopted the strategy for a more effective fight against child sexual abuse.

[54] See CTOC/COP/WG.4/2021/2 for more examples.

B. Possible responses

78. When it comes to the prevention of serious forms of violence against children, including online abuse and exploitation, primary prevention measures may include ensuring the prohibition by law of this form of violence against children, implementing comprehensive, tailored prevention strategies and programmes and promoting research and data collection. States have largely let the technology industry take voluntary, self-regulatory measures to prevent crimes such as online trafficking in persons or online child sexual exploitation.[55] This has not proved enough, and States should develop strong regulatory frameworks and oversight to stop the current impunity. States could adopt safety measures such as age and consent verification of persons involved in explicit videos on common platforms and age verification of their viewers, as well as easier procedures for content removal when harmful and illicit material is detected.

79. Secondary prevention measures may include enhancing the ability and capacity of the criminal justice system to respond to online child abuse and exploitation. This entails establishing effective detection and reporting mechanisms, offering effective protection to child victims of violence, ensuring the investigation and prosecution of incidents of violence against children and improving criminal proceedings, enhancing cooperation among various sectors, ensuring that sentencing reflects the serious nature of violence against children, and strengthening the capacity and training of professionals. Specific measures may include the identification and removal of content by involving private entities such as communication service providers and the establishment of protocols with technology companies and online platforms so that unlawful content is not deleted by communication service providers but is instead forwarded to law enforcement agencies for investigation and prosecution.[56] Private-public partnerships need to be strengthened to ensure further accountability of platforms hosting illegal content.

80. These actions can be complemented by advocacy and awareness-raising initiatives, including specialized capacity-building of all relevant actors involved in the detection and removal of online content and awareness-raising and educational initiatives addressed to children themselves, in order to empower them to act as agents of change for their own protection.

C. Questions for consideration

81. The Commission may wish to discuss the following questions:

(a) Does the current international legal framework sufficiently address issues related to information and communications technology and online child abuse, exploitation and trafficking in persons?

(b) How can Member States strengthen the key role of the justice system, including through cooperation with other relevant stakeholders, in preventing and responding to online child abuse and exploitation?

(c) Which regulatory frameworks and measures should be adopted to enhance the detection and reporting of online child sexual abuse, exploitation or trafficking in persons, address the demand for such content and increase the liability of technology companies and online platforms for hosting unlawful and harmful materials?

[55] Organisation for Security and Co-operation in Europe, Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, “Policy responses to technology-facilitated trafficking in human beings: analysis of current approaches and considerations for moving forward” (Vienna, 2022), pp. 2–6.

[56] Ibid., p. 3.

(d) What capacity-development activities are currently needed for law enforcement entities to be able to effectively investigate online child abuse, exploitation and trafficking in persons, and collect relevant electronic evidence?

(e) How can international organizations such as UNODC assist Member States in strengthening international cooperation to prosecute and hold perpetrators of child online abuse and exploitation accountable?

(f) How can international organizations such as UNODC assist Member States in strengthening public-private partnerships to ensure accountability for private companies and receive access to evidence and data relevant for investigations and prosecutions?

(g) What innovative strategies and measures exist for promoting the engagement of children and young people in their own protection from online abuse, exploitation and trafficking in persons?