United Nations E/CN.15/2011/2

Economic and Social Council

Distr.: General
31 January 2011

Original: English

Commission on Crime Prevention and Criminal Justice
Twentieth session
Vienna, 11-15 April 2011
Item 4 of the provisional agenda*
Thematic discussion on protecting children in a digital age: the misuse of technology in the abuse and exploitation of children

Discussion guide for the thematic discussion on protecting children in a digital age: the misuse of technology in the abuse and exploitation of children

Note by the Secretariat

Summary

The present note has been prepared by the Secretariat as a discussion guide for the thematic discussion of the Commission on Crime Prevention and Criminal Justice at its twentieth session. In its decision 2010/243, entitled "Report of the Commission on Crime Prevention and Criminal Justice on its nineteenth session and provisional agenda and documentation for its twentieth session", the Economic and Social Council decided that the prominent theme for the twentieth session of the Commission would be "Protecting children in a digital age: the misuse of technology in the abuse and exploitation of children". The Commission, in its decision 18/1, entitled "Guidelines for the thematic discussions of the Commission on Crime Prevention and Criminal Justice", decided that the discussion should be based on a discussion guide including a list of questions to be addressed by participants, such guide to be prepared by the Secretariat.

The present guide proposes a series of questions for discussion by the Commission, outlines some issues for shaping the discussion and further elaborates upon the relevant subthemes. It describes the main challenges to effective protection of children in a digital age and makes suggestions for improving such protection.

* E/CN.15/2011/1.

V.11-80434 (E) 010311 020311

I. Introduction

A. Guidelines for the thematic discussions of the Commission on Crime Prevention and Criminal Justice

1. The Economic and Social Council, in its decision 2010/243, entitled "Report of the Commission on Crime Prevention and Criminal Justice on its nineteenth session and provisional agenda and documentation for its twentieth session", decided that the prominent theme for the twentieth session of the Commission would be "Protecting children in a digital age: the misuse of technology in the abuse and exploitation of children".

2. The Commission on Crime Prevention and Criminal Justice, in its decision 18/1, entitled "Guidelines for the thematic discussions of the Commission on Crime Prevention and Criminal Justice", 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, such guide to be prepared by the Secretariat in the six official languages of the United Nations, not later than one month in advance of the session. In that resolution, the Commission also:

(a) Urged Member States and regional groups to put forward their nominations for panellists not later than two months in advance of each session of the Commission and decided that the panellists would be selected one month in advance of the session, bearing in mind that five seats on the podium would be allocated to the regional groups;

(b) Decided that independent experts, such as private sector representatives and academics, may be invited, pursuant to the rules of procedure of the Economic and Social Council, to contribute to the thematic discussions of the Commission, taking into account, inter alia, regional considerations and legal frameworks;

(c) Decided also that the guidelines for the thematic discussions of the Commission would be as follows:

(i) Each thematic discussion should be moderated under the authority of the Chairperson and the bureau of the Commission and should be conducted under the Chairperson's authority as set out in the rules of procedure of the functional commissions of the Economic and Social Council;

(ii) Introductory presentations by panellists should be brief, not exceeding 10 minutes, and panellists should be encouraged to share their presentations in advance;

(iii) Participants should be prepared to focus on the theme and subthemes agreed upon by the Commission in order to allow for a dynamic and interactive exchange during the thematic discussion;

(iv) In their statements, speakers should touch upon national experiences of their Governments in relation to the subthemes. Within the framework of the rules of procedure applicable to the Commission, the views of intergovernmental and non-governmental organizations would be welcome;

(v) Statements by participants should be limited to a maximum of five minutes;

(vi) The moderator should intervene to enforce time limits and should keep a list of speakers but may use his or her discretion to select speakers according to the thrust of the discussion;

(vii) At the end of the thematic discussion, the Chairperson should prepare a summary including the most salient points discussed.

B. Subthemes for the thematic discussion

3. At an intersessional meeting held on 27 January 2011, the Commission endorsed the following subthemes, upon recommendation by the extended Bureau of the Commission at its first meeting, on 11 January 2011:

(a) Nature and scope of the problem of misuse of new technologies in the abuse and exploitation of children:

(i) Typology of risks and threats to children and how children are affected by new technologies, including social networks and text-messaging;

(ii) Global trends and patterns in the misuse of new technologies in the abuse and exploitation of children, and how the reporting and analysis of such trends and patterns can be facilitated through improved data collection;

(iii) The role of the private sector in new technologies and other relevant areas and how the private sector can help address the problem of abuse and exploitation of children;

(iv) Understanding the impact of cybercrime on child victims, the varying impact of different offences and which offences pose greater risks;

(b) Responses to the problem of misuse of new technologies in the abuse and exploitation of children:

(i) Preventing the misuse of digital media and new technologies in the abuse and exploitation of children, including through education and awareness-raising (considering, as appropriate, cyberethics, cybersafety and cybersecurity in relation to children), situational prevention (targeted messages for children, service providers etc.) and technical prevention (modifications to technologies to deter crime or facilitate enforcement);

(ii) Development and harmonization, as applicable, of criminal justice and other measures to prevent and investigate cybercrime offences targeting children and prosecute offenders;

(iii) Enhancing regional and international cooperation and exploring ways and means to cooperate with the private sector, including the possible elaboration of codes of conduct for industry;

(iv) Enhancing national capacities through adequate and evidence-based technical assistance.

4. The present note has been prepared by the Secretariat as a discussion guide. It proposes a series of questions for discussion by the Commission and provides background information to support the discussion.

II. Misuse of technology in the abuse and exploitation of children

A. Issues for discussion

5. It is suggested that Member States consider including in their delegations to the Commission at its twentieth session experts on the misuse of technology, cybercrime and the abuse and exploitation of children to address the issues proposed for discussion.

1. Questions on risks and threats to children

6. Questions on a typology of risks and threats to children might include the following:

(a) How are the risks and threats to children affected by the presence of new technologies?

(b) Has the development of information and communications technologies actually expanded the overall market for online child sexual abuse and exploitation materials, and if so, by what means, or has it simply brought an age-old problem into the spotlight?

(c) What is the impact of social networks, text-messaging and an increasing use of mobile devices and location-based services on new forms of illegal behaviour that harms children?

(d) Is there a typology of online child sexual abuse and exploitation?

2. Questions on global trends and patterns

7. Questions on global trends and patterns in the misuse of new technologies in the abuse and exploitation of children might include the following:

(a) How could the reporting and analysis of such trends and patterns be facilitated through improved data collection?

(b) What are the various sources from which information about trends and patterns in offending might be obtained, including not only criminal justice statistics and victim surveys but also private sector and technological sources, child-welfare sources and other sources?

(c) How could the amount of scientific data on child abuse in the virtual world be increased?

(d) How can information about the presence and roles played by information and communications technologies be gathered separately in the reporting and recording of cases involving online child sexual exploitation and abuse?

(e) In what way could relevant data be collected so as to ensure a response from Member States and enhance coordination in international data collection exercises?

(f) A global picture of the problem and of rates, trends and patterns can be obtained only by using information from both developed and developing countries.

Given the challenges faced by developing countries in reporting and recording criminal justice statistics in general, what sources of data could be accessed in these countries, and what sorts of technical assistance could be used to assist them in collecting and providing the necessary data?

(g) How can general data on rates, trends and patterns with respect to the availability and use of information and communications technologies in countries of all levels of social, economic and technological development be used to provide a background context for the analysis of data concerning the specific problems relating to child victimization?

(h) How could a comprehensive data management system be set up to provide better access to existing databases and facilitate information-sharing among law enforcement agencies?

(i) Would one central database with links to existing national databases be an effective system?

(j) What measures could overcome the difficulties of establishing databases and of updating and effectively sharing information through it?

3. Questions on the role of the private sector

8. Questions on the role of the private sector in new technologies and other relevant areas in order to address the problem of abuse and exploitation of children might include the following:

(a) What role can the private sector play in the prevention of offences, including in the areas of:

(i) Technical prevention through better technical security measures to alert parents or authorities to suspicious activities?

(ii) Situational crime prevention through the development of best practices and the education or training of employees, parents, children at risk and other identified groups; social prevention through general awareness-raising about the nature of the problem and what society as a whole can do to prevent and combat it?

(b) How can the private sector assist in enabling the implementation of protection measures installed on the users' side?

(c) How can the private sector assist investigators and law enforcement authorities in investigating child abuse and child exploitation cases, and what domestic and international safeguards are needed to protect both the integrity and independence of the criminal justice system and the rights of those involved in any way (i.e. suspects, victims, witnesses and others)?

(d) Shall the involvement be based on mandatory obligations or a self-regulatory approach?

(e) What role could the private sector play in assisting with the preservation, transfer and use of evidence (e.g. by authenticating files)?

(f) What role can the private sector play in helping to locate and identify victims and to mitigate the harm caused by victimization?

(g) Which measures can be implemented to ensure that involvement of the private sector follows a balanced approach?

4. Questions on the impact of cybercrime on child victims

9. Questions on the impact of cybercrime on child victims might include the following:

(a) Are there certain crimes of which children are more likely to become victims?

(b) If there are such offences, what are the reasons for that situation? (This might include a discussion about whether the offenders are specifically targeting children to make use of their limited level of experience in recognizing criminal conduct.)

(c) Has the spread of information and communications technologies affected the likelihood that children in some regions will be victimized through the creation of new illicit markets, and if so, how?

(d) Are there differences between the nature and impact of victimization in cases where technologies are involved and cases where they are not? If so, what effects on victims do specific uses of technology tend to produce?

(e) How can data about the impact of cybercrime on child victims be collected? Is such information contained in crime statistics?

(f) Have children developed countermeasures and strategies to deal with such offences? What are these measures and strategies, and can they be adapted to other areas of crime in which children are victims?

(g) How do technologies make the tracing and identification of victims more difficult, and how can this be remedied so as to increase the ability to locate and assist child victims, both within Member States and globally?

5. Questions on preventing the misuse of new technologies in the abuse and exploitation of children

10. Questions on preventing the misuse of digital media and new technologies in the abuse and exploitation of children, including through education and awareness-raising, situational prevention and technical prevention, might include the following:

(a) How can the protection and support of children who are witnesses of crime be enhanced?

(b) What are the implications for lawmakers and law enforcement authorities of different forms of online child sexual abuse and exploitation?

(c) What is the role and mission of surveillance platforms in the Internet and of the round-the-clock national units?

(d) What measures can be put in place to ensure that criminal justice authorities keep abreast of changes in technology and trends associated with the abuse and exploitation of children? Are there any specialized law enforcement units

in charge of combating these crimes and exchanging related practices and information?

(e) What good practices exist in relation to awareness-raising and dissemination of information about the abuse and sexual exploitation of children in the context of Internet use, including cyberethics, cybersafety and cybersecurity?

(f) What national measures and responses have there been to raise awareness to prevent and protect children from all types of abuse and exploitation in connection with the misuse of information and communications technologies, including the promotion of good practises and lessons learned to achieve those purposes?

(g) What experience has there been in putting in place a range of technical means of prevention for the different types of crimes against children committed through the misuse of information and communications technologies?

(h) What means are available to ensure stricter control over the users of chat rooms and social networks on the Internet? Could such controls be an effective step to combat sexual exploitation of children through the use of the Internet?

(i) What kind of security measures exist or need to be developed to protect children using online applications, including social networks and chat rooms? What measures can be taken to prevent accidental access to child sexual abuse content?

(j) How can prevention by means of early identification and treatment of perpetrators, including medical and psychological treatment, be improved?

(k) How could technological means be improved to ensure the physical security of children using the Internet?

6. Questions on criminal justice and other measures

11. Questions on criminal justice and other measures to prevent, investigate and prosecute perpetrators of cybercrime targeting children might include the following:

(a) To what extent do existing international/regional instruments include criminal justice provisions to combat the misuse of technology in connection with the sexual abuse and exploitation of children, trafficking in persons, especially children, and child pornography? Are there mechanisms for their implementation?

(b) Would harmonization of the key features of the different relevant conventions be effective in combating these crimes, or would assessment of the existing legal instruments and suggestions for potential improvements be more constructive?

(c) What practices and techniques have proved effective in investigating such crimes and gathering and preserving related evidence?

(d) What is the extent of the involvement of organized criminal groups in the abuse and exploitation of children? Would the United Nations Convention against Transnational Organized Crime[1] be an appropriate legal basis for addressing these issues? How can the Convention be used to address these activities?

---

[1] United Nations, *Treaty Series*, vol. 2225, No. 39574.

(e) What measures can be taken in order to modify provisions to seize and secure digital evidence?

(f) What tools to facilitate the detection and investigation of such crimes can be put in place? How can existing tools be improved?

7. Questions on regional and international cooperation

12. Questions on regional and international cooperation and ways to cooperate with the private sector might include the following:

(a) In what ways could the cooperation and input of States at the national level and between relevant authorities be developed in order to build the capacity needed to provide such information and data?

(b) What ways are there to promote closer collaboration between relevant entities in the public sector and the private sector in developing and implementing preventive and reactive measures in combating the misuse of technology in the abuse and exploitation of children?

(c) How can the United Nations Office on Drugs and Crime (UNODC) improve its partnerships with other parties involved, including regional and international agencies and organizations, Governments, the Internet industry and other private sector entities, law enforcement authorities and financial investigators? What needs to be done to enable coordination of ongoing initiatives in various forums with a view to articulating more coherent and concerted approaches and action?

(d) Would it be effective to impose obligations on the Internet industry to further regulate and control their services? Should there be consequences when such entities fail to act to fulfil obligations? Some of the following could be considered:

(i) Establishing legal requirements for the development and use of technological tools;

(ii) Elaboration of a manual of ethics for the Internet industry;

(iii) Establishing legal liability, whether criminal, civil or administrative;

(iv) Loss of the licence to operate if obligations are not fulfilled:

(e) What are the main difficulties encountered when cooperating with other States in combating the misuse of technology in the abuse and exploitation of children?

(f) What measures and tools have proved effective in fostering law enforcement cooperation and the exchange of information?

(g) How could cooperation in the monitoring of the Internet be strengthened?

(h) How can regional and international cooperation to prevent and counter the abuse and exploitation of children be further enhanced, including the seizure and confiscation of assets deriving from illicit activities?

(i) What measures are in place to enhance national coordination to facilitate international cooperation?

(j) What types of cooperation (bilateral, regional and/or international) could be used effectively, and how would these relate to each other?

(k) How could the provisions of the Organized Crime Convention on international cooperation be applied in the context of combating the sexual exploitation of children?

(l) How can requests for international cooperation be processed in a faster and therefore more effective manner?

(m) How can effective international methods of combating online child sexual abuse content be achieved? Some of the following could be considered:

(i) Combating online child sexual abuse and exploitation should be part of the work of agencies already set up to combat organized crime and corruption and child sexual abuse through the misuse of technology;

(ii) The need for a unified international law enforcement approach to tackling commercial child sexual abuse websites with significant longevity, which continuously change servers and national police jurisdictions, with a view to ensuring the investigation of the distributors and the removal of the content;

(iii) Industry self-regulation and support of national hotlines, supported by the necessary relevant legislation;

(iv) Adoption at the national and international levels of "notice and take-down" joint measures by hotlines and industry to enable all web-hosting companies and Internet service providers to remove child sexual abuse content from their networks, regardless of whether they are members of a national centre or participate in a hotline;

(v) The provision of a comprehensive, dynamic list of currently active child sexual abuse websites to Internet service providers, mobile operators, search providers and filtering companies to facilitate the blocking at the network level of access to such content, to protect Internet users from exposure to it and to minimize the perpetuation of the sexual abuse of the child victims through repeated viewing;

(vi) Establishment of an industry code of practices to achieve online sector support of recognized good practices, aims and principles;

(vii) International efforts by domain name registries and relevant authorities to enable the de-registration of domains associated with child sexual abuse;

(viii) Participation of all hotlines in a centralized (for example, regional) database listing child sexual abuse sites, in order to enable optimum data-sharing, comprehension of the scale of the problem and the effective allocation of resources;

(ix) Sharing of comprehensive international data, intelligence and expertise, as well as the pooling of ideas to help combat the cross-border nature of these crimes;

(x) The need for the establishment of recognized international good practices to ensure unified responses and enhance the availability of the Internet in safe

conditions in developing countries so that opportunities for the abuse of such online services can be minimized in a proactive fashion;

(n) What needs to be done to further promote international cooperation in combating the misuse of technology in the abuse and exploitation of children? Could the following be useful to that end:

(i) Creation of working groups with operational skills at the regional level?

(ii) Pursuing standardization of legislation and procedures for investigating systems?

(iii) Training of staff?

8. Questions on capacity-building and technical assistance

13. Questions on capacity-building and technical assistance might include:

(a) What good practices exist for strengthening the capacities of law enforcement officials and prosecution services to deal with the misuse of technology?

(b) What practices and techniques have proved effective in training law enforcement and other relevant agencies in the detection and investigation of the misuse of technology in the abuse and sexual exploitation of children?

(c) What are the priority technical assistance needs in the field of preventing and combating crimes against children, in particular in the light of the lack of capacity and expertise in this area?

(d) How can capacity-building proceed more effectively? What types of training materials are needed and how can it be provided sufficiently? Some of the following might be considered:

(i) Technical training on computer forensics for investigators, including on specific forensic software;

(ii) Legal training for police, prosecutors and judges to raise awareness of possibilities and limitations with respect to the application of local laws and to the activities of international organizations;

(iii) Creation of discussion groups for law enforcement officials for a fast and effective exchange of experiences, best practices and challenges encountered, in order to provide further assistance with regard to national legislation and ways and means to further harmonize and improve that legislation;

(e) How can UNODC help Member States upgrade their capacity to efficiently address child abuse and exploitation through the misuse of technology? How can UNODC facilitate the delivery of specific technical assistance activities in this field?

B. Background

1. Overview

14. The worldwide proliferation of new information and communications technologies has given rise to new and increasingly frequent forms of crime, a situation that poses threats not only to the confidentiality, integrity and availability of computer systems but also to the safety and security of their users, especially children. Over the past two decades, use of the Internet and other related information and communications technologies has increased significantly in all parts of the world. Today, nearly two billion people worldwide use the Internet and its services. Although this development has facilitated access to information and communication between people and has been beneficial for children in many ways, it also poses new risks and threats to children's safety, personal development and well-being.

15. The Internet has increased the range, volume and accessibility of sexually abusive imagery, including child pornography, by creating an environment for its proliferation and creating and expanding a market for its consumption. Owing to the increasing bandwidth of Internet connections, enabling the rapid exchange of files and its much wider reach, the Internet has become the primary medium for the exchange of child pornography. As a consequence, children are being victimized multiple times, for once an image is online, it can be viewed by an unlimited number of persons. There is a persistent core of commercial child sexual abuse websites, generating profits for organized criminal groups. But there are not only commercial child pornography websites. Whereas just a few years ago, most websites were commercial, today many people who access child pornography are trading images on the Internet using applications such as non-commercial peer-to-peer networks. That, in turn, poses challenges for law enforcement authorities that pay increasing attention and devote increasing resources to combating online sexual offences. In addition, use of such applications and peer-to-peer networks limits the possibilities of tracing money flows to assist in investigations.

16. Information and communications technologies have also created new virtual environments for children and youth. Owing to the rapid development of Internet technologies, social networking (Myspace, Facebook) has become increasingly popular as a means of social communication. One feature of that new type of social interaction is the disclosure of private information, as more and more children, especially teenagers, use such networks as a kind of substitute diary, a situation which can be abused by perpetrators and may thus facilitate new forms of criminality that need to be addressed. Perpetrators can take advantage of these social networks and chat rooms to recruit their victims, by approaching them using false identities or "chat names" to lure them into physical meetings, through solicitation or "grooming" (the increasingly worrying phenomenon of adults meeting in person, and sexually abusing, children that they have previously encountered in Internet chat rooms or game sites). In this way, online and offline abuse are being connected. Finally, sexual abuse and exploitation in the converged online/offline environments are likely to be linked to other types of sexual abuse and exploitation such as trafficking and sex tourism.

17. The expansion of the Internet has also posed many new challenges with respect to the commercial exploitation of children. With regard to e-commerce, especially the shift towards online retailing, equivalents of the traditional safeguards against the commercial exploitation of children have yet to be found for the virtual environment of the Internet. Children and young people constitute a significant target market for a large number of different businesses. They are potential customers in their own right and also have a great influence on the spending of their parents and wider family.[2] The implications for children as consumers have yet to be fully examined.

2. Mandate and work of the United Nations Office on Drugs and Crime

18. The most common forms of computer-related crimes fall within the definition of the Organized Crime Convention as they are transnational, involve organized criminal groups and are committed with the aim of achieving a material or financial benefit. In this regard, an interpretative note to article 2 of the Convention indicates that the words in article 2, subparagraph (a), of the Convention "in order to obtain, directly or indirectly, a financial or material benefit" should be interpreted broadly, to include, for example, crimes in which the predominant motivation may be sexual gratification, such as the receipt or trade of materials by members of child grooming rings, the trading of children by paedophile rings or cost-sharing among ring members.[3] The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, is also relevant to the issue of the use of new information technology, including the Internet, to facilitate child abuse and exploitation.

19. The General Assembly, in its resolution 64/179, entitled "Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity", drew attention to the emerging policy issues identified in the report of the Secretary-General (A/64/123), namely, piracy, cybercrime, sexual exploitation of children and urban crime, and invited UNODC to explore, within its mandate, ways and means of addressing those issues.

20. The specific issue of child sexual abuse and exploitation is underlined in Commission resolution 16/2, entitled "Effective crime prevention and criminal justice responses to combat sexual exploitation of children". In that resolution, the Commission encourages Member States to take appropriate measures, consistent with their international obligations and national legislation, to prevent and make efforts to eliminate the use of mass media and information technologies, including the Internet, to facilitate or commit child sexual exploitation offences.

21. The issue of the use of information and communication technologies, including the Internet, for child sexual abuse and exploitation was included in the discussion at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Salvador, Brazil, from 12 to 19 April 2010. In the Salvador

---

[2] Children's Charities' Coalition on Internet Safety (2010) Briefing on the Internet, e-commerce, children and young people. Available from www.chis.org.uk.

[3] *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (United Nations publication, Sales No. E.06.V.5), p. 17.

Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World,[4] endorsed by the General Assembly in its resolution 65/230, Member States called upon the private sector to promote and support efforts to prevent child sexual abuse and exploitation through the Internet.

22. In 2005, in the Bangkok Declaration on Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, endorsed by the General Assembly in its resolution 60/177, Member States, in particular, reaffirmed the fundamental importance of implementation of existing instruments and the further development of national measures against cybercrime, and welcomed the efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime. Member States also invited the Commission on Crime Prevention and Criminal Justice and the United Nations Office on Drugs and Crime to examine the feasibility of providing assistance to Member States in addressing computer-related crime under the aegis of the United Nations in partnership with other similarly focused organizations.

3. Legal instruments and mechanisms

23. The Convention on the Rights of the Child, adopted by General Assembly in its resolution 44/25 and which entered into force on 2 September 1990, does not criminalize child pornography but provides an important foundation for the protection of children. The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography was adopted by the General Assembly in its resolution 54/263 and entered into force on 18 January 2002. Currently, 193 States are parties to the Convention, and 142 States are parties to the above-mentioned Optional Protocol. The Convention spells out the basic human rights of all children everywhere, including the right to survival; the right to develop their potential to the fullest; the right to protection from harmful influences, abuse and exploitation; and the right to participate fully in family, cultural and social life. The four core principles of the Convention are non-discrimination; devotion to the best interests of the child; the right to life, survival and development; and respect for the views of the child. The Convention protects children's rights by setting standards in health care; education; and legal, civil and social services. States parties to the Convention are obliged to develop and undertake all actions and policies in the light of the best interests of the child.

24. The United Nations Convention against Transnational Organized Crime was adopted by the General Assembly in its resolution 55/25 and entered into force on 29 September 2003. Currently, 158 States are parties to the Convention. The Convention commits States parties to introducing a range of measures for the strengthening of mutual legal assistance, extradition and other forms of judicial and law enforcement cooperation to combat all serious crime. Although the Convention applies only in cases where an organized criminal group is involved, defining a criminal group as such if one of its objectives is to generate a financial or other material benefit, most serious cybercrime falls within the scope of the Convention. The meaning of the term "financial or other material benefit" is relatively broad and encompasses, for example, identity-related crimes committed online, where stolen

[4] A/CONF.213/18, chap. I, resolution 1.

or fabricated identification or identity information is treated as an illicit commodity and bought, sold or exchanged. The treatment of a subject matter as a form of illicit commodity that is bought, sold or exchanged by organized criminal groups would also apply to the use of information technologies, in particular the Internet, in child sexual abuse and exploitation. Under article 29 of the Convention, parties are required to develop specific training programmes for law enforcement personnel (including prosecutors and investigating magistrates). Article 29, paragraph 1 (h), states that such programmes shall deal with methods used in combating transnational organized crime through the use of computers, telecommunications networks or other forms of modern technology.

25. The Trafficking in Persons Protocol was adopted by the General Assembly in its resolution 55/25 and entered into force on 25 December 2003. According to article 2 of the Protocol, the purpose of the Protocol is to prevent and combat trafficking in persons especially woman and children, protect and assist the victims of such trafficking and to promote international cooperation among States parties in order to meet those objectives. There are currently 142 parties to the Protocol.

26. The Council of the European Union framework decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography is aimed at harmonizing the laws and regulations of the States members of the European Union with respect to police and judicial cooperation in criminal matters in order to combat the sexual exploitation of children and child pornography. The framework decision introduces a framework of common provisions on criminalization, sanctions, aggravating circumstances, assistance to victims and jurisdiction.[5] Under the framework decision, punishable conduct that constitutes an offence related to child pornography, whether undertaken by means of a computer system or not, includes the production, distribution, dissemination or transmission, supplying or making available, acquisition and possession of child pornography. In 2010, the European Union published a proposal for a directive on combating the sexual abuse, sexual exploitation of children and child pornography repealing framework decision 2004/68/JHA. The directive includes a broad criminalization of child pornography as well as a provision dealing with grooming.

27. The 2001 Council of Europe Convention on Cybercrime and its Explanatory Report were adopted by the Committee of Ministers of the Council of Europe at its 109th session, on 8 November 2001. The Convention was opened for signature in Budapest on 23 November 2001 and entered into force on 1 July 2004. The Convention deals with crimes committed via the Internet and other computer networks. Its main objective is to pursue a common criminal policy aimed at the protection of society from cybercrime, especially by adopting appropriate legislation and fostering international cooperation. Article 9 of the Convention deals with offences related to child pornography. The Convention provides a legal basis for cooperation in a context that is much broader than one comprising only States members of the European Union, as the Convention is open for accession to other States as well. Currently, 30 countries have ratified the Convention.

---

[5] More information on European Union legislation to combat trafficking in persons is available from http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_trafficking_in_human_beings.

28. The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse was adopted and opened for signature by the States members of the Council of Europe, non-member States that participated in the elaboration of the Convention and States members of the European Union on the occasion of the twenty-eighth Conference of European Ministers of Justice, held in Lanzarote, Spain, on 25 and 26 October 2007. The Convention entered into force on 1 July 2010. Among other measures, the Convention criminalizes the use of the new technologies, in particular the Internet, to sexually harm or abuse children, for example by knowingly obtaining access, through information and communication technologies, to child pornography or grooming. In that regard, the Convention goes beyond the standards defined by the Council of Europe Convention on Cybercrime.

4. Current challenges in protection of children from the misuse of information and communication technologies

29. With the expansion of new information and communications technologies, law enforcement authorities are also faced with new kinds of challenges in investigating crimes involving the misuse of those technologies. Investigations are in most cases complex and time-consuming, because they are often coordinated across jurisdictions and target networks of offenders using varying levels of security. For global partnerships to disrupt and investigate such sites, Governments, the Internet industry, police, hotlines, non-governmental organizations, children's charities, educators, psychologists and financial investigators must all work together in order to effect change and minimize the continued sexual abuse of children through the use of technology. Moreover, such criminal activities highlight the significance of fostering the best possible cooperation between law enforcement authorities and Internet service providers.

30. One of the unique features of the Internet that attracts both children and teenagers to disclose much of their most private information — and attracts perpetrators who try to take advantage of such information — is the anonymity that the Internet affords. At the same time, that anonymity creates one of the biggest problems for law enforcement authorities investigating online child abuse, exploitation, child pornography and other crimes committed through the misuse of communication technologies. Owing to the fact that the Internet and its services are not bound by jurisdictions or national borders, the investigation of crimes involving new technologies very often have a global dimension, making international judicial cooperation especially important. Also, identifying a user requires the analysis of traffic data such as Internet Protocol addresses, which in turn requires the assistance of Internet service providers. A further issue is whether the analysis of uploaded content requires the assistance of hosting providers. Hosting providers have a greater ability to identify illicit content, because they are not limited by reliance on public search engines or by access restriction systems implemented by the client, and they have the ability to control access to information outside of jurisdiction boundaries.

31. Adding to the challenges, it is not unusual for more than one Internet service provider to be involved in the process, and perpetrators may use services provided free of charge, such as advertisement-sponsored web pages, because such services generally do not require formal registration. However, the monitoring and analysis of data is indispensable for the investigation of these offences in order to obtain

digital evidence, which may disappear if not preserved within minutes. Such data might even be deleted automatically after the transaction has been finalized. That situation dramatically limits the time frame for successful investigations, which require timely and effective cooperation between national law enforcement authorities and Internet service providers.

32. To be able to respond to those challenges, law enforcement agencies need the right legal instruments and specific training to be able to identify offenders and collect the evidence required for criminal proceedings. Major advances in the area of forensic science and technology and the increased use of science in judicial proceedings have made a significant contribution to the fight against crime in the past decade. New technologies are helping to continually enhance the work performed at crimes scenes and in forensic laboratories. Such advances have enhanced the efficiency of the criminal justice system in detecting crimes, convicting offenders and exonerating innocent people. However, law enforcement authorities in some countries suffer from the lack of available forensic software to collect evidence, conduct keystroke logging and decrypt or recover deleted files in investigations involving new information and communication technologies. The development of modern information and communications technology is largely controlled by private operators, and there is a significant deficit in the exchange of expertise, information and best practices between the public and the private sector. Law enforcement authorities are not provided with the necessary technical training and expertise, resources, capacity and equipment such as sufficient investigating management software and databases to be able to meet and adjust to the constantly changing and evolving methods employed by criminals who use information and communications technology to commit their crimes.

5. Preventive measures

33. The misuse of technology in the abuse and exploitation of children is an issue affecting the vast majority of States. Although there are numerous legal instruments and mechanisms available at the national, regional and international levels to fight the offline abuse and exploitation of children, very little is in place to counter these kinds of crimes committed online or through the use of information and communications technologies. That situation underlines the great need for specific legislation and other legal and technical measures and assistance to counter the abuse and exploitation of children committed through the misuse of information and communication technologies. Existing legislation and other preventive measures designed to protect children from abuse and exploitation now have to be altered and amended where necessary to provide an appropriate framework for the fight against the abuse and exploitation of children with an online component.

(a) National legislation

34. Member States have adopted or are in the process of developing an array of measures, including amending existing and establishing new legislation to close gaps in the criminalization of different forms of child abuse in connection with new information and communications technologies, including online child pornography and child grooming.

(b) Other prevention measures and initiatives

35. Multiple approaches and measures have been launched at the national and regional levels to deal with the challenges posed by these new types of crime. For example, some States have started to implement special training for law enforcement authorities, judges and prosecutors to address the challenges in investigating Internet-related crimes and to provide intensified technical assistance for police authorities in order to promote and improve police investigations on the Internet and ensure swift and efficient prosecution (see E/CN.15/2009/14).

36. In the United Kingdom of Great Britain and Northern Ireland, the Internet Watch Foundation is operating a "notice and take-down" scheme in order to remove child sexual abuse content on networks in the United Kingdom. However, work remains to be completed to speed up the process. The Internet Watch Foundation has also established a hotline specializing in combating online child sexual content, including a free and anonymous reporting mechanism for the public to report their exposure to potentially criminal child sexual abuse content and established international partnerships to share data, intelligence and tactics in order to combat the cross-border nature of such crimes.[6] Another example of hotlines are those operated as part of the International Association of Internet Hotlines that was founded in 1999 under the European Commission Action Plan for a Safer Internet for the period 1999-2004.

37. Several initiatives have been launched to raise awareness with regard to safety settings for online activity, including the Children's Charities' Coalition on Internet Safety and the Child Online Protection initiative of the International Telecommunication Union.

6. International cooperation

38. The International Criminal Police Organization (INTERPOL) has established a database of child abuse images enabling police to use sophisticated computer software to compare images and share information at the international level in order to identify visual clues in the images, such as recurring backgrounds. The database contains approximately 300,000 images of child abuse taken from the Internet.

39. The Organized Crime Convention and the Trafficking in Persons Protocol promote international cooperation among 158 States parties and provide a legal framework for mutual legal assistance and extradition. The Convention also encourages the use of bilateral and multilateral agreements in situations where the Convention itself cannot be used as a legal basis.

40. The Child Exploitation Tracking System is an application that Microsoft Canada has developed in partnership with Canadian and international law enforcement agencies to help police combat the online exploitation of children, including child pornography and luring. It is designed to enable collaboration and information-sharing among police services and increase the effectiveness of investigations by providing tools to store, search, share and analyse the large volumes of investigative information.

---

[6] See www.iwf.org.uk/resources/trends.

41. An idea originally put forward by the Group of Eight Subgroup on High-Tech Crime led to the inclusion in the Council of Europe Convention on Cybercrime of a provision for parties to designate 24/7 contact points in order to facilitate and accelerate international cooperation in all cases of cybercrime where speed is crucial for the success of the investigation. The structure is designed to enable law enforcement authorities to immediately identify experts in other countries and obtain immediate assistance in computer-related investigations.