7 May 2014

English only

Commission on Crime Prevention and Criminal Justice
Twenty-third session
Vienna, 12-16 May 2014
Item 7 of the provisional agenda*
World crime trends and emerging issues and responses in the field of crime prevention and criminal justice

Assessment of the needs of States for training in the investigation of offences against children committed by using new information and communications technologies

The present document was prepared pursuant to Economic and Social Council resolution 2011/33 on prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. In that resolution, the Economic and Social Council requested the United Nations Office on Drugs and Crime, taking into account, where appropriate, relevant data collected by the expert group, to design and carry out an assessment of the needs of States for training in the investigation of offences against children committed by using new information and communications technologies and, on the basis of the results of that survey, to design a training and technical assistance programme to assist Member States in combating such offences more effectively, subject to the availability of resources and not duplicating the efforts of the International Criminal Police Organization (INTERPOL).

* E/CN.15/2014/1.

V.14-03041 (E)

Assessment of the needs of States for training in the investigation of offences against children committed by using new information and communications technologies

Introduction

1. In addition to a study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children,[1] Economic and Social Council resolution 2011/33 requested the United Nations Office on Drugs and Crime (UNODC) to design and carry out an assessment of the needs of States for training in the investigation of offences against children committed by using new information and communications technologies (ICTs).[2] The Council further requested UNODC, on the basis of the results of that assessment, to design a training and technical assistance programme to assist Member States in combating such offences more effectively, subject to the availability of resources and not duplicating the efforts of the International Criminal Police Organization (INTERPOL).

2. The present document contains both the requested assessment of the needs of States for training in the investigation of offences against children committed by using ICTs, as well as proposed elements for a training and technical assistance programme to assist Member States in this area.

3. In resolution 2011/33, the Council requested that both the study of the effects of new information technologies on the abuse and exploitation of children and the assessment of training needs in this area should take into account, where appropriate, relevant data collected by the open-ended intergovernmental expert group to conduct a comprehensive study on the problem of cybercrime.[3] The report on the second meeting of the expert group on cybercrime, held in Vienna from 25 to 28 February 2013, noted that there was broad support for capacity-building and technical assistance, and for the role of UNODC in that regard.[4] Accordingly, the assessment of training needs contained in this document makes reference to information contained in the Comprehensive Study on Cybercrime prepared by UNODC in February 2013 for the consideration of the open-ended intergovernmental expert group on cybercrime (hereinafter the "Cybercrime Study").[5]

4. Information gathering on the needs of States for training in the investigation of offences against children committed by using ICTs was facilitated by an informal expert group meeting held in September 2013.[6] The informal expert group meeting brought together international experts from the fields of law enforcement, research,

---

[1] Contained in document E/CN.15/2014/CRP.1.

[2] ECOSOC resolution E/2011/33 on "Prevention, protection and international cooperation against the use of new information technologies to abuse and/or to exploit children" (28 July 2011).

[3] Ibid., paras. 15 and 16.

[4] Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 25 to 28 February 2013. 1 March 2014. UNODC/CCPCJ/EG.4/2013/3.

[5] Available at: www.unodc.org/documents/commissions/CCPCJ_session22/13-80699_Ebook_2013_study_CRP5.pdf.

[6] Experts present at the meeting are listed at the Annex to this assessment.

industry and civil society. The informal expert group discussed the scope of possible training needs, including obstacles in the identification of crimes; collection of evidence; victim assistance; protection and cooperation; conducting efficient joint operations; international cooperation; and government structures to combat these forms of crime.

Needs in the identification of crimes

5. The informal expert group considered that one of the greatest obstacles to the detection of technology-facilitated offences against children was a lack of dedicated staff trained in all aspects of ICT-facilitated child abuse and exploitation cases. This observation coincides with information from the Cybercrime Study, which noted that less than one per cent of all police are specialists in cybercrime.[7] Skilled and dedicated personnel, perhaps organized into inter-agency task forces or units, can aid in all aspects of investigation and prosecution of ICT-facilitated child abuse and exploitation cases, including developing expertise on handling digital evidence and conducting image analysis; studying offender profiles; interviewing and assisting child victims and witnesses; developing networks to facilitate cooperation across jurisdictions and borders; elaborating appropriate counter strategies for common defences in judicial proceedings; and learning how to clearly and persuasively present technical evidence to judges and juries.

6. Training for personnel in such units or task forces may best take place on an inter-agency basis, with a view to building informal relationships and establishing working protocols. In addition, support to dedicated units for ICT-facilitated child abuse and exploitation crimes can ensure the continuous availability of technically skilled human resources.

7. The informal expert group also noted that investigations of ICT-facilitated child abuse and exploitation offences tended to be reactive in nature, rather than proactive, due to, in part, the limited possibilities to undertake undercover investigations. The most common methods of such undercover investigations consist of law enforcement agents posing as children, virtually entering chat rooms, setting up websites that purport to display child sexual abuse material, or joining child sexual abuse communities purporting to be a consumer.

8. Many members of the informal expert group noted that undercover operations are not permitted in many countries, creating an obstacle for law enforcement authorities, as they cannot interact with possible offenders, who groom children online with the intent of abuse. First and foremost, States require a clear legal framework that regulates such operations,[8] which are legally complex in nature. For instance, many offenders may require their victims or co-perpetrators to engage in initiation rites, such as the uploading of child sexual abuse material, which is meant to dissuade or detect undercover law enforcement agents. Policies and laws must therefore exist that clearly set out procedures for law enforcement officers who encounter such situations. In addition, undercover operations are most useful where States have clear criminalization provisions for inchoate crimes, such as attempts or preparation for an offence. In the absence of such legal provisions, investigators cannot arrest would-be offenders until and unless the crime is completed, such as

[7] UNODC. 2013. Comprehensive Study on Cybercrime, p. 154.

[8] Bose, A., 2013.

when the victim is actually abused or exploited. This situation, in turn, considerably undermines the purpose of anti-child abuse and exploitation laws, policies and operations.[9]

Needs in investigative capabilities and electronic evidence

9. The informal expert group identified the most significant obstacle to effective investigative capabilities as the lack of ability to obtain stored or real-time data on traffic or content, or subscriber information. As noted in the Cybercrime Study, the interplay between law enforcement and Internet service providers is particularly complex.[10] Service providers often hold valuable evidentiary material that is volatile due to its electronic nature. Such evidence can include subscriber information, billing invoices, some connection logs, location information and communication content. The volatility of electronic evidence requires timely response to requests from investigators and the ability to request specialized investigative actions.

10. In addition, national legal obligations and private sector data retention and disclosure policies vary widely by country, industry and type of data. Most commonly, service providers require due legal process for disclosure of customer data. Accordingly, court orders may be required to obtain electronic evidence from service providers. In some cases, however, law enforcement may be able to obtain data directly. This can be facilitated by informal partnerships between law enforcement authorities and service providers. In this respect, the informal expert group noted that some countries lacked expedited procedures for preserving computer data, as well as formal or informal relationships with electronic service providers.

11. Several members of the group further highlighted that the law enforcement agencies of their countries lacked basic sufficient material resources, including access to reliable electricity, computer hardware, computer software and the Internet. Specialized training for prosecutors and judges in handling digital evidence and in understanding issues common to technology-facilitated child abuse and exploitation cases was also identified as a need by the informal expert group. This corresponds with information contained in the Cybercrime Study, which noted that 40 per cent of all countries for which information was available did not offer any cybercrime-specific training for judges, while another quarter only offered basic training.[11] One member of the expert group specified that prosecutors should receive training together with investigators. In particular, training was required to identify Internet protocol (IP) addresses; adapt foreign reports that use Greenwich Mean Time to local time zones; safeguard the integrity of data throughout the chain of custody; determine the relevant foreign authorities to obtain timely responses to requests for assistance; and effectively use experts to analyse digital evidence.

---

[9] Wei, W., 2010. *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System*. Available at https://www.iwf.org.uk/assets/media/resources/IWF%20Research%20Report_%20Development%20of%20an%20international%20internet%20notice%20and%20takedown%20system.pdf .

[10] See UNODC, 2013. P. 144.

[11] Ibid., p. 177.

12. The informal expert group recommended that trainers carry out specific pre-training needs assessments, especially for needs in digital forensics training and tailored to the legal, cultural, and economic context of a requesting country. Finally, the group recommended that a single entity take a leadership role in keeping track of ongoing training to avoid duplication of efforts; share and build on the knowledge; collaborate with trainers in future programmes; and exchange materials and findings with others in the field.

Needs in international cooperation

13. Obstacles to the effective investigation of ICT-facilitated child abuse and exploitation offences can become magnified when requests for information and assistance are received from abroad. This may especially be the case with respect to multi-jurisdictional operations or when countries do not have an established relationship that is based either on treaty arrangements or reciprocity. Some countries may represent jurisdictional "seats" for a large number of electronic service providers and can receive significant numbers of requests compared with available capacities.

14. The informal expert group indicated that the lack of standard operating procedures for requests involving digital evidence may pose a major obstacle. The group also noted the challenge of slow response times and a lack of channels to obtain assistance with urgent mutual legal assistance requests. Such needs correspond with information contained in the Cybercrime Study, which identified the current international cooperation picture as one with response times for formal mechanisms of the order of months.[12] Long-time scales in international cooperation may be related to reliance on traditional formal channels of communication that typically necessitate the involvement of multiple authorities in the communication chain. For instance, all countries included in the Cybercrime Study reported using post or diplomatic letters for mutual legal assistance in cybercrime cases.

15. With a view to strengthening international cooperation processes, the group further identified a lack of contacts in requested countries as a problem for investigators, and emphasized that there was a need for training on executing assistance requests in order to ensure the receipt of corresponding data, as well as a need for training on the general nature and elements of international investigations.

Needs related to victim assistance, protection and cooperation

16. In terms of victim assistance, protection and cooperation, the informal expert group noted a need for greater emphasis on training for law enforcement and criminal justice authorities. The main deficiencies identified were the absence of standard protocols for supporting victims through the investigative process, techniques for interviewing victims, and the collection and preservation of victim-related evidence. As child victims constitute a particularly vulnerable group of persons impacted by crime, they need to be attended to in a sensitive, balanced manner. Untrained law enforcement officers may unintentionally act insensitively towards victims and thus cause them more psychological harm. In addition, the informal expert group emphasized that law enforcement agents often required training on the dynamics related to sexual abuse and exploitation within families.

[12] Ibid., p. 197.

Needs related to awareness-raising

17. Another obstacle to successfully combatting ICT-facilitated crimes against children is a lack of awareness among children, families and society at large, particularly in respect of whether conduct — such as cyberbullying or sexual harassment — constitutes a criminal offence or not. It is crucial that both children and adults understand when and how to report an offence. As the Cybercrime Study noted, cybercrime acts most frequently come to the attention of law enforcement authorities through reports by individual or corporate victims. In this respect, one global private sector survey suggests that 80 per cent of individual victims of core acts of cybercrime do not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment and perceived reputational risks for corporations.[13] The informal expert group indicated that both public and private sectors require a channel to alert law enforcement authorities about ongoing and potential offences. The group also highlighted the importance of electronic service providers working cooperatively with law enforcement to identify and prevent the most common offences committed on their networks.

18. The informal expert group highlighted the need for education programmes to promote awareness, and to support wider prevention of cybercrime. The provision of training to children directly to aid them in independently identifying online perpetrators, as well as all forms of sexual victimization, was identified as a priority. The group also suggested increased provision of information to parents on the ways that ICTs impact their children's daily life and on the crucial preventative role that parents can play by communicating with their children, setting boundaries around the use of technological devices and paying attention to their children's concerns and interests, in order to identify warning signs of abuse or exploitation. The continued importance of public awareness-raising campaigns, including those covering emerging threats, and those targeted at other specific audiences besides parents, was also highlighted by Governments, private sector entities and academic institutions in the Cybercrime Study. Public-private partnerships are essential in this regard, which already exist in a number of countries for prevention purposes, by informal agreement and by legal basis. Actions covered by such partnerships complement those of law enforcement and can help mitigate damage to victims.

Needs related to policy and coordination

19. The informal expert group identified that the development of an overarching national law, policy or strategy against ICT-facilitated child abuse and exploitation with clear priorities and targets can greatly contribute to a sustainable, coordinated effort against such offences. As noted in the Cybercrime Study, only 40 per cent of responding countries indicated the existence of any such national initiative in respect of cybercrime in general. A national law, policy or strategy to prevent and combat ICT-facilitated child abuse and exploitation can also set the groundwork for the establishment of an inter-agency coordination group for the purposes of both operational coordination of government responsibilities, as well as aiding the further promulgation of policy and legal frameworks.

---

[13] Ibid., http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V13/807/73/PDF/V1380773.pdf?OpenElement, p.10.

20. The group noted that there was an urgent need for senior officials in the criminal justice field to be made aware of the severity of the problem of technology-facilitated child exploitation and abuse and the importance of digital evidence in investigations, noting that most law enforcement agents do not realize that almost every criminal investigation involves the use of computers.

Other training needs

21. In terms of practical design of trainings, the informal expert group recommended that trainers execute specific pre-training needs assessments, especially on digital forensics training needs, tailored to the legal, cultural, and economical context of a requesting country. In addition, trained and/or specialized judicial staff is needed to effectively and adequately address these crimes. Finally, the group recommended that a single entity should take on a leadership role in tracking ongoing international training initiatives, in order to avoid duplication of efforts; share and build on existing knowledge; collaborate with trainers on future programmes; and share materials and findings with all available experts.

Proposed Elements of a UNODC Technical Assistance Programme to Prevent and Combat Technology-Facilitated Child Abuse and Exploitation

Introduction

22. Pursuant to Council resolution 2011/33, and in response to the needs of States identified by the informal expert group, this section proposes elements of a UNODC training and technical assistance programme to assist Member States in combating ICT-facilitated child abuse and exploitation offences more effectively (the "Programme"). In accordance with Council resolution 2011/33, the Programme would be implemented subject to the availability of resources and not duplicating the efforts of the International Criminal Police Organization (INTERPOL).

23. A UNODC training and technical assistance programme in this area would have synergies with, but also be conceptually distinct from, the current UNODC Global Programme on Cybercrime. Pursuant to, inter alia, General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolution 22/8, UNODC works, on the basis of the needs of requesting States, to strengthen partnerships for technical assistance and capacity-building to counter cybercrime with Member States, relevant organizations, the private sector and civil society. Under the Global Cybercrime Programme, UNODC has delivered training on digital forensics and investigations at the regional level in Eastern Africa, as well as in countries in Central America. Activities are also planned to commence in countries of South-Eastern Asia in the course of 2014.

24. A training and technical assistance programme on combatting ICT-facilitated child abuse and exploitation offences pursuant to Council resolution 2011/33 may leverage activities already undertaken by UNODC through the Global Programme on Cybercrime. Support to the establishment and training of law enforcement cybercrime units under the Global Programme on Cybercrime, for example, may also specifically include support to an Internet crimes against children subunit —

combining expertise on digital forensics with child abuse investigation, image analysis, undercover investigation and child protection approaches. In this respect, a UNODC Programme on combatting ICT-facilitated child abuse and exploitation would bring together the work of Organized Crime Branch (with a law enforcement and organized crime perspective) and Justice Section (with a focus on the United Nations standards and norms for crime prevention and criminal justice, including Justice for Children approaches, as well as the Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime). In addition, UNODC would seek to implement programme activities in close cooperation with INTERPOL and UNICEF, as well as other actors relevant in the prevention and combatting of online child sexual abuse, with a view to ensuring maximization of impact and resources, whilst avoiding duplication of efforts.

Proposed Programme activities

Law enforcement training

25. The programme would provide law enforcement agencies of requesting countries with training on specialized methods for investigating online crimes against children. Whilst some overlap exists with digital forensics approaches used in the investigation of other cybercrime cases, online child abuse investigation techniques may differ in a number of respects. These include as regards the particular skills required for image analysis, matching and identification; with respect to the perspective of child safeguarding and protection; and with respect to the conduct of undercover operations.

26. Training activities for police officers would therefore cover a range of relevant issues such as the types of technology-facilitated crimes committed against children; offender and victim profiles and their relevance to the investigation; international image searching and checking; investigation approaches; and providing assistance and protection to victims.

27. Image identification through checking of national and international image databases is especially important in investigations involving ICT-facilitated child abuse and exploitation. Old pictures and videos may be edited or manipulated and subsequently recirculated, causing investigators to waste time and resources on investigating cases which have already been solved in the past if careful image checks are not made. Investigation-based training would be delivered in cooperation with INTERPOL and could include support to a live investigation, as well as training in use of the International Child Sexual Exploitation Image Database.

28. The programme would deliver training for specialist law enforcement officials responsible for interviewing and safeguarding child victims and witnesses of abuse and exploitation. This may include, in particular, training on the rights of children to be treated with dignity and compassion; to be protected from discrimination; to be informed; to be heard and to express their views and concerns; to privacy; to be protected from further hardship or victimization; to safety; to reparation; and to the necessary assistance and support, including financial, legal, counselling, health, social and educational services, physical and psychological recovery services and other services necessary for the child's reintegration. Child protection aspects would be delivered in cooperation with UNICEF and other relevant organizations.

29. In addition to training of officers and investigators, the programme would support law enforcement authorities in establishing the necessary administrative structures for the effective operation of police ICT-facilitated child abuse units. These can include administrative decrees establishing the functions of a unit, as well as the development of standard operating procedures to ensure the sustainability, efficiency and psychological wellbeing of officers.

30. Support would also be provided to strengthening cooperation of law enforcement authorities with electronic service providers. This may be achieved through the facilitation of meetings with representatives of service providers to discuss current mechanisms and possible formal and informal means of cooperation. Such means may include not only access to digital evidence, but also mechanisms for monitoring and reporting of child sexual abuse material, as well as deletion of criminal content.

31 Finally, training may also be provided on human rights aspects of law enforcement investigations into ICT-facilitated child abuse and exploitation acts, including with respect to international standards on freedom of expression and privacy, and the extent of permitted interference under international law.

International cooperation and training for prosecutors and judges

32. Support would be provided to law enforcement, prosecutors and central authorities responsible for preparing and sending, and receiving and implementing mutual legal assistance requests in matters involving ICT-facilitated child abuse and exploitation. In particular, training may be delivered on means — including informal cooperation means — to secure the expedited preservation of computer data; on the effective preparation of mutual legal assistance requests involving digital evidence; and on the use of UNODC tools, such as the Directory of Competent National Authorities and the MLA Writer Tool, including its new digital evidence module presently under development.

33. The programme may employ existing cooperation platforms presently supported by UNODC, such as REFCO (Network of Central American Prosecutors against Organized Crime) and WACAP (Network of West African Central Authorities and Prosecutors against Organized Crime) to deliver training to prosecutors. This may include training on strengthening understanding of investigations with a technological component; on attributing and confirming the age of victims in order to avoid dismissal of cases; on proving the authenticity of images and other media files; on elaborating appropriate counter strategies for common defences in judicial proceedings; and on determining the level of coercion in the creation of self-generated pictures and videos, if relevant. Training aimed at improving the technical and legal skills of prosecutors may also be adjusted for use in information sessions for judges who handle cases of technology-facilitated crimes against children.

34. Finally, the programme would deliver training for prosecutors and judges on protection considerations where child victims or witnesses are required to testify during the criminal justice process. This may include training on preparation of video or remote-link testimony, as well as possibilities for judicial protection orders where child victims or witnesses may be the subject of intimidation, threats or harm.

Awareness-raising

35. Public awareness-raising campaigns, including those targeted at specific audiences such as children, continue to be critical as a "first-line" approach in the prevention of ICT-facilitated child abuse and exploitation.

36. Taking into account the extensive range of material already available, the programme would develop an awareness-raising toolkit for Member States with specific emphasis on ICT-facilitated child abuse and exploitation to assist in the implementation of national campaigns. The toolkit would include templates for a variety of campaign products. These may include a public service announcement, a website, a general information brochure, a poster, a child-focused leaflet, web banners and a social media pack. Intended audience for the material would include children themselves, reached directly and through youth organizations and schools, as well as parents, guardians, teachers, youth leaders and other caregivers. The toolkit would be made available online and in physical format (such as via DVD/CD) to facilitate dissemination and allow Member States to tailor content to national needs. As countries adapt materials, the toolkit would be expanded to include examples of locally-adapted materials from other Member States.

37. The toolkit would initially be translated into the six official United Nations languages with potential for further translation into other languages. Materials would be disseminated by UNODC's Advocacy Section through UNODC field offices and applicable media channels.

Sustainability

38. UNODC would deliver assistance in requesting countries in close cooperation with relevant government stakeholders in each specific sector. Mechanisms to ensure the sustainability of support may include the accreditation of training courses with national police academies and other relevant institutions, as well as securing standard operating protocols and specialist staffing arrangements within law enforcement authorities.

Proposed next steps

39. The challenges of ICT-facilitated child abuse and exploitation are unlikely to be overcome in the near future. Growing levels of global interconnectivity offer increasing and rapidly evolving opportunities for criminal activities. As requested by Council resolution 2011/33, it is critical that UNODC seek to support Member States in this area, through a sustainable and effective training and technical assistance programme.

40. A sustainable response will require commitment from all stakeholders in order to build awareness; allocate sufficient human and technological resources to prevent and combat these types of crimes, establish supportive government structures; enable proactive investigations; and train practitioners on gathering, preserving, presenting and delivering judgements based on electronic evidence.

41. UNODC stands ready, together with relevant international partners, including INTERPOL and UNICEF, to begin implementation of a training and technical assistance programme to assist Member States in combating ICT-facilitated child

abuse and exploitation offences more effectively. Next steps will involve the development of a full project document, based on the assessment of the training needs of States in this area, as well as the elements proposed in this document. This may then be followed by a resource mobilization phase and initial roll-out of activities in selected pilot regions or subregions, according to need and upon Member State request for assistance.

Annex

List of Experts

The assessment of needs greatly benefited from the inputs of the following expert practitioners in the fields of law enforcement, prosecution, academia, the private sector and civil society:

Maria Teresa Aguirre, Paraguay

Anjan Bose, ECPAT International

John Carr, Online Child Safety Consultant

Carla Della Donne, Argentina

Guillermo Gallarza, International Center for Missing and Exploited Children

Paul Gillespie, Kids' Internet Safety Alliance (KINSA)

Jorge Luis San Lucas Gonzalez, Ecuador

Susie Hargreaves, Internet Watch Foundation

Apichart Hattasin, Thailand

Jenny Jones, GSMA

Lata Kallychurn, Mauritius

Carla Licciardello, International Telecommunications Union (ITU)

Bjørn-Erik Ludvigsen, Norway

Nelly Montealegre, Mexico

Michael Moran, INTERPOL

Andrew Morling, United Kingdom

Omashani Naidoo, South Africa

Heila Niemand, South Africa

John Peacock, New Zealand

John Penn, Adobe

Cristian Perella, Facebook

Anders Persson, Sweden

Ethel Quayle, COPINE Project

Patrick Redling, Virtual Global Task Force

Jonathan Rouse, Australia

Seila Samleang, APLE Cambodia

Vanessa Fusco Simoes, Brazil

Hana Snajdrova, Organization for Security and Cooperation in Europe (OSCE)

Clara Sommarin, United Nations Children's Fund (UNICEF)

Oran Sukkasem, Thailand

Joe Sullivan, Mentor Forensic Services

Daniel Szumilas, Germany

Janis Wolak, Crimes against Children Research Center

The Organized Crime and Illicit Trafficking Branch of UNODC is also grateful for the input of UNODC staff members Margaret Akullo, Adam Palmer, Anna Giudice Saget, and Alexandra Souza Martins.