United Nations CTOC/COP/WG.3/2015/2

Conference of the Parties to the United Nations Convention against Transnational Organized Crime

Distr.: General
18 August 2015

Original: English

Working Group on International Cooperation
Vienna, 27-28 October 2015
Item 2 of the provisional agenda*
Gathering and sharing electronic evidence

Gathering and sharing electronic evidence

Background paper prepared by the Secretariat

I. Introduction

1. Crimes involving electronic evidence present unique challenges for those authorities entrusted to give appropriate responses to it both domestically (law-makers, investigators, prosecutors and judges) and at the level of international cooperation.

2. In general terms, electronic evidence can include any data generated or stored in digital form whenever a computer is used. It includes information manually entered into an electronic device by an individual, information generated in a computational transaction or a response to a request by an individual, where an electronic device generates information acting as an automaton, or information produced and stored where a device processes information within its matrix. Electronic evidence is, therefore, any information captured, generated or maintained in databases, operational systems, applications programmes, computer-generated models which extrapolate outcomes, electronic and voice mail messages and even instructions held inertly within a computer memory bank.[1]

3. The present paper has been prepared by the Secretariat with a view to providing background information on key concepts and aspects pertaining to electronic evidence and to aid the discussions of the Working Group on the relevant agenda item of its meeting.

---

* CTOC/COP/WG.3/2015/1.

[1] Ireland Law Reform Commission, "Documentary and Electronic Evidence", Consultation paper, December 2009, p. 8.

V.15-05868 (E) 280815 310815

II. The gathering and sharing of electronic evidence: areas for consideration and responses at the national and international levels

4. Both the gathering and sharing of electronic evidence are closely linked and, consequently, national legislation and regional and international agreements or arrangements often provide for investigative powers to collect electronic evidence and cooperation mechanisms to share it.

A. Gathering electronic evidence

1. National legal frameworks

5. Traditional criminal procedural laws typically contain provisions on the gathering and admissibility of evidence. When it comes to evidence in electronic form, computer data and electronic records can be altered easily. Thus, the gathering and handling of electronic evidence should guarantee its integrity, authenticity and continuity during the entire time period between its seizure and its use in trial.

(a) Legal powers to collect and handle electronic evidence

6. National investigative powers play a key role in gathering electronic evidence. As stated in the UNODC Cybercrime Study, in order to conduct effective investigations and gather electronic evidence, States may enact procedural legislation granting powers to relevant law enforcement authorities. Investigative powers can range from applying traditional procedural powers, broadly interpreted general investigative powers, general investigative powers tailored to apply to a range of cyber-specific measures and comprehensive investigative powers implemented to obtain electronic evidence.[2]

7. As further highlighted in the Cybercrime Study, the examination of the legal basis for investigative powers used in crimes involving electronic evidence reveals considerable diversity in approaches at national level. Such approaches are first related to the extent to which “traditional” powers can be interpreted to apply to non-tangible data, as well as the extent to which legal authority exists for particularly intrusive measures, such as remote forensic investigations.

8. Nonetheless, while legal powers vary, a good degree of consensus among the States that reported for the purposes of the Cybercrime Study appears to exist on the types of investigative measures that should be available for gathering electronic evidence. Such measures may include the expedited preservation of computer data; orders for stored content data; orders for stored traffic data; orders for subscriber information; real-time collection of content data; real-time collection of traffic data;

---

[2] UNODC, Comprehensive Study on Cybercrime: Draft — 2013, prepared by UNODC for the consideration of the Expert Group to Conduct a Comprehensive Study on Cybercrime (www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf), Chapter 5, p. 125.

search for computer hardware or data; seizure of computer hardware or data; trans-border access to a computer system or data; and use of remote forensic tools.[3]

9. For law enforcement authorities to effectively investigate and gather electronic evidence related to cybercrime, cooperation with other relevant actors, including from the private sector, has gained particular importance over the last years. Overall, Internet Service Providers (ISPs) play an important role in the accessibility of electronic evidence. National privacy laws can also impact the ability of ISPs to share information with relevant authorities during an investigation. By way of example, States may enforce restrictions on what data can be accessed, impose time limits, have "probably cause" requirements, and prosecutorial and judicial oversight.[4] As a result of the privacy-based protections found in national legislation, ISPs may be bound to withhold information concerning a subscriber's personal information, content data and traffic data. In addition to national laws for laws, international human rights law sets specific standards for the privacy rights of persons subject to law enforcement investigations.

10. The Council of Europe "Guidelines for the cooperation between law enforcement and internet service providers against cybercrimes" was adopted in response to the importance of ISPs in gathering electronic evidence. The guidelines are meant to help law enforcement authorities and ISPs to properly structure their interactions when dealing with cybercrime issues. The guidelines are intended to be flexible and apply in any country in accordance with national legislation and respect for fundamental rights of citizens. Law enforcement authorities and ISPs are encouraged, among others, to engage in information exchange; promote a culture of cooperation; develop written procedures for mutual cooperation; consider establishing formal partnerships; and protect fundamental rights of citizens.[5]

(b) Capacity-building for law enforcement and criminal justice systems in handling electronic evidence

11. Electronic evidence is, by its very nature, fragile. It can be altered, damaged or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

12. Capacity-building at the level of national law enforcement and criminal justice systems is therefore critical. While the majority of countries have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence, in many countries those structures are underfunded and suffer from a lack of capacity. As digital evidence becomes increasingly pervasive in the investigation of "conventional" crime, so law enforcement authorities may need to make clear distinctions between, and establish clear workflows for, cybercrime investigators and digital forensic laboratory capacity. Front-line law enforcement

---

[3] Examples of national laws on those investigative measures can be found in the Cybercrime Repository (http://cybrepo.unodc.org) and SHERLOC (http://sherloc.unodc.org).

[4] Cybercrime Study, Chapter 5, p. 134.

[5] Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, available at www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

officers may also increasingly need to acquire and deploy basic skills, such as those used to produce a sound forensic image of an electronic storage device.

13. As new technological developments such as anonymizing networks, high-grade encryption and virtual currencies become commonplace in offences involving electronic evidence, investigators will also have to adopt new strategies. Law enforcement authorities may, for example, look to strengthen partnerships with academic research groups that focus on the development of technical methodologies in areas such as the characterization and investigation of virtual currency transactions.[6] Investigators may also need to consider how special investigative techniques, such as surveillance, undercover operations, using informants and controlled delivery in the case of the sale of illicit goods online, may be used alongside Internet investigation and digital forensic techniques for gathering sensitive and fragile electronic evidence. Overall, it is clear that capacity-building for law enforcement and criminal justice actors on combating cybercrime and/or crime involving electronic evidence will be an ongoing and continuous process, as technology and criminal innovations continue at a rapid pace.[7]

(c) The role of specialized cybercrime structures or units: domestic approaches

14. The specialization of national law enforcement agencies in the investigation of cybercrime and/or crimes involving electronic evidence is becoming increasingly common and plays a crucial role in facilitating the processes of gathering, analysing and sharing electronic evidence. This specialization is primarily linked to the particular nature of cybercrime, which presents specific challenges related to offence definitions, applicability of laws, and evidence gathering and analysis. The level of 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.[8] In addition, given the growing prevalence of electronic devices, the Internet and global connectivity in daily life, electronic evidence, such as text messages, e-mails and Internet browsing data have become standard in many "conventional" criminal investigations.[9] As a result, there is also a mounting need for law enforcement at all levels — whether local or national — to have at least basic capabilities for investigating cybercrime.

15. The most commonly cited area for "technical assistance interventions" in the Cybercrime Study was generally that of cybercrime investigative techniques. Of those countries requiring assistance, 60 per cent indicated that this was needed by law enforcement agencies.[10] States reporting for the purposes of the Cybercrime

---

[6] See, for example, Sarah Meiklejohn and others, "A fistful of bitcoins: characterizing payments among men with no names", in Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference (New York, ACM, 2013).

[7] Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, Background paper prepared by the Secretariat for Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation, A/CONF.222/12, paras. 37-38.

[8] Cybercrime Study, Chapter 5, p. 152.

[9] See footnote 7 above, A/CONF.222/12, para. 16.

[10] Cybercrime Study, Executive Summary, p. xxiii.

Study further indicated that, in many cases, local police stations transferred cybercrime cases to a specialized national-level law enforcement lead.[11]

16. Specialized cybercrime structures or units within law enforcement agencies can make it easier for States to concentrate limited resources in a single place in order to build specialized investigative techniques and to adequately gather and analyse electronic evidence, including conducting digital forensic examinations. At the same time, such structures or units may provide training for local law enforcement agencies, coordinate national responses to cybercrime, facilitate cooperation among partners involved in the investigations, and target forms of cybercrime that may be of particular concern to a State, such as child online abuse, identity-related crime, Internet frauds and scams, etc.

(d) Admissibility of electronic evidence in courts

17. Once electronic evidence is gathered and shared, it would ideally be admissible in criminal proceedings. The law of evidence traditionally relied on paper records, though oral testimony and physical objects have always been part of the courtroom proceedings. However, the increasing relevance of electronic evidence in criminal proceedings present challenges previously unknown and therefore the Cybercrime Study was a "mapping exercise" to reflect national legal approaches with regard to the admissibility of such evidence in criminal courts.

18. In this context, 85 per cent of responding countries reported that electronic evidence was admissible in criminal proceedings. The greater number of countries that admit electronic evidence reported that such evidence is treated in the same way as physical evidence. A percentage of under 40 per cent of countries reported the existence of a legal distinction between electronic and physical evidence. Very few countries reported the existence of special evidentiary laws governing electronic evidence. For those that did, laws covered areas such as legal assumptions concerning ownership or authorship of electronic data and documents, as well as circumstances in which electronic evidence may be considered authentic.[12]

2. International cooperation

19. Crimes involving digital evidence, present unique challenges to international cooperation. Owing to the volatile nature of electronic evidence, international cooperation in cybercrime matters requires a timely response and the ability to request specialized investigative actions, including preservation and production of data by private sector providers. Common challenges in requesting such data from another jurisdiction include delays in responding to requests, a lack of commitment and flexibility from the authority from which evidence is requested, the form in which evidence is provided to the requesting jurisdiction and whether it can be used in criminal proceedings, and the differing definitions of criminal offences between jurisdictions.[13]

---

[11] Cybercrime Study, Chapter 5, p. 118.

[12] Cybercrime Study, Chapter 6, pp. 165-167.

[13] UNODC Comparative study on current practices in electronic surveillance in the investigation of serious and organized crime, p. 9 (www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf).

20. While a number of modes of informal law enforcement cooperation exist, including "24/7" networks, countries continue to rely heavily on traditional formal judicial means, in particular bilateral mutual legal assistance instruments, to obtain extraterritorial electronic evidence, with over 70 per cent of countries using formal mutual legal assistance requests.[14] Response times for such mutual legal assistance requests involving investigation of cybercrime are typically about 150 days. Such timescales may often fall outside of service provider data retention periods or may enable perpetrators to permanently destroy key digital evidence.

21. Effective international cooperation in cases involving digital evidence therefore requires mechanisms for the expedited preservation of data pending consideration of further investigative measures. International cooperation in cases involving digital evidence may also be enhanced by common approaches for formulating requests for specific forms of evidence, including network evidence, connections logs and forensic images.

22. Some existing multilateral instruments establish mechanisms that are aimed at facilitating access to data for law enforcement agencies, such as points of contact that are available around the clock in cybercrime investigations, trans-border access to stored computer data with consent or where publicly available and urgent requests for mutual assistance.

23. For example, under the Council of Europe Cybercrime Convention, "24/7" points of contact shall facilitate, or, if permitted by domestic law and practice, directly carry out: (i) provision of technical advice; (ii) preservation of data; and (iii) collection of evidence, provision of legal information, and locating of suspects.

24. A number of international agreements address areas related to the gathering of electronic evidence. By way of example, the Council of Europe Convention on Cybercrime specifies that the scope of procedural provisions contained in the Convention shall apply to powers and procedures for the purposes of collecting evidence in electronic form of a criminal offence.

25. The Common Market for Eastern and Southern Africa (COMESA), Cybersecurity Draft Model Bill (2011) contains provisions relating to ISPs. Provisions include monitoring obligations (art. 17); voluntary supply of information (art. 17(b)); take-down notifications (art. 16); liability of access providers (art. 12), caching (art. 13), hosting (art. 14) and hyperlink providers/search engines (art. 15). In addition, the European Union Directive 2000/31/EC and the ITU/CARICOM/CTU (i) Model Legislative Texts on Cybercrime/e-Crimes and (ii) Electronic Evidence contain similar, but fewer, provisions than the COMESA Model Bill.

26. Informal cooperation may take place between law enforcement agencies to gather electronic evidence from other jurisdictions. Such cooperation can facilitate various measures for obtaining extraterritorial evidence, including search and seizure; preservation of computer data, orders for computer data; real-time collection of data; remote forensic tools; and direct law enforcement access to extraterritorial data.[15]

---

[14] Cybercrime Study, Executive Summary, p. xxv.

[15] Cybercrime Study, Chapter 5, pp. 126-133.

27. Law enforcement may increasingly need to find pioneering ways of collaborating on transnational cybercrime investigations. The involvement of entities such as the INTERPOL Global Complex for Innovation[16] and the European Police Office (Europol) European Cybercrime Centre (EC3)[17] in coordinating and supporting transnational investigations may prove especially important in that regard. Other forums and initiatives, such as the Global Conference on Cyberspace, have also offered the opportunity for countries to consider innovative responses in the area of international cooperation against cybercrime.

28. Cloud computing also poses an increased challenge for international cooperation because computer services are increasingly being moved to geographically distributed servers and data centres, making it difficult to determine where electronic evidence is "located".[18] By way of example, a Google-user may access data stored or processed in North America, South Eastern Asia, or Northern or Western Europe.[19]

B. Sharing electronic evidence

1. National legal frameworks

29. Some States have instituted domestic legislation that address sharing evidence through international cooperation. By way of example, many States have domestic legislation on mutual assistance in criminal matters that may also be utilized to share electronic evidence.

2. International cooperation

30. To facilitate the sharing of electronic evidence between jurisdictions, States may enter into bilateral, regional and international agreements. Such agreements may contain provisions relating to assistance in the preservation of computer data; assistance for the seizure, access to, collection of and disclosure of computer data; trans-border access to computer data; provision of unsolicited information and exchange of information; and general mutual legal assistance (MLA) requests.[20] The provisions included in such agreements constitute primary sources of law that cover both the rights and the obligations of the parties to the agreements, thus subjecting the parties to binding legal terms. However, not all States require a formal treaty for judicial cooperation to share electronic evidence and, instead, may provide assistance on the basis of reciprocity or comity.

31. A review of regional and international agreements demonstrates the various forms available for States to share electronic evidence. Such forms of cooperation include general principles of international cooperation; general mutual legal assistance; mechanisms for expedited assistance; assistance for the preservation of computer data; assistance for the seizure/access to/collection of/disclosure of computer data; trans-border access to data; and provision of unsolicited

---

[16] www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.
[17] www.europol.europa.eu/ec3.
[18] Cybercrime Study, Chapter 7, p. 216
[19] Cybercrime Study, Chapter 7, pp. 216-217.
[20] Cybercrime Study, Annex 3, pp. 273-274.

information/exchange of information. The following agreements contain a range of the aforementioned forms of cooperation:

United Nations, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000);

Commonwealth of Independent States, Agreement on Cooperation in Combating Offences related to Computer Information (2001);

Council of Europe, Convention on Cybercrime and Additional Protocol to the Convention of Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2001);

Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007);

Economic Community of West African States (ECOWAS), Draft Directive on Fighting Cybercrime within ECOWAS (2009);

League of Arab States, Arab Convention on Combating Information Technology Offences (2010);

Shanghai Cooperation Organization, Agreement on Cooperation in the Field of International Information Security (2010); Common Market for Eastern and Southern Africa (COMESA);

Cybersecurity Draft Model Bill (2011);

African Union, Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (2012);

European Union, Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment (2001);

European Union, Council Framework Decision 2005/222/JHA on attacks against information systems (2005);

European Union, Proposal COM (2010) 517 final for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (2010).

32. The primary methods used to share electronic evidence are traditional cooperation, such as formal MLA requests. A number of bilateral, regional and international agreements exists that address MLA procedures. Many of the regional and international cybercrime instruments listed above include provisions on MLA. MLA procedures and requests are predominantly dictated by regional and bilateral agreements. Examples of regional agreements on MLA include the Association of Southeast Asian Nations (ASEAN) 2004 Treaty on Mutual Legal Assistance in Criminal Matters and the Council of Europe's 2000 European Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union.

33. In view of the often volatile and easily contaminated nature of electronic evidence, timely responses required for such evidence may not always be provided through formal cooperation mechanisms. Thus, informal cooperation mechanisms can also be used and "24/7" networks, in particular, hold a considerable potential for streamlining such informal cooperation or even facilitating — at a later stage — formal cooperation. However, the availability of investigative actions which are

possible through informal cooperation can vary significantly. A major hurdle sharing electronic evidence through informal cooperation is that many countries prohibit the use of evidence obtained through informal mechanisms in the context of judicial proceedings.[21]

34. Countries that make use of informal cooperation noted, while reporting for the purposes of the Cybercrime Study, that related mechanisms are dependent upon the existence of a competent and well-organized foreign counterpart. Countries observed that this is more likely when informal law enforcement cooperation is governed by some form of agreement. A number of countries reported that informal cooperation is therefore conducted on the basis of regional and bilateral agreements, through use of networks established by international and regional organizations and institutions; with the assistance of embassies and consulates; as well as through private networks among law enforcement officers.

35. To that end, article 27 of the United Nations Convention against Transnational Organized Crime (UNTOC) contains provisions on law enforcement cooperation and encourages States to consider entering into bilateral or multilateral agreements or arrangements allowing for cooperation between different law enforcement bodies. In addition, States have also instituted various laws on law enforcement cooperation, including exchange of information, joint investigations, electronic or other forms of surveillance, etc.

36. While some countries report to direct police-to-police cooperation, others focus primarily on informal cooperation through INTERPOL channels. INTERPOL has bureaus in 190 countries often linked with national law enforcement agencies.[22] As a result, the bureaus may support informal relationships, thus enhancing the likelihood of successful alternatives to formal international cooperation procedures.

37. A number of challenges to both formal and informal cooperation procedures regarding electronic evidence in criminal matters can impede both the gathering and sharing of such evidence. Examples include divergences in the scope of cooperation provisions contained in multilateral and bilateral instruments, a lack of response time obligation, multiple informal law enforcement networks and variance in cooperation safeguards.[23]

III. Tools developed by the United Nations Office on Drugs and Crime

38. During the past years, UNODC has produced a number of tools, which address the topic of electronic evidence from different perspectives, disciplines and mandates. In this regard, UNODC tools encompass a mutually-reinforcing spectrum of knowledge, which is often gathered through extensive consultations with Member States and relevant stakeholders. From research-based analysis on specific forms of crimes to electronic platforms providing direct access to legal resources, UNODC

---

[21] Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, Chapter 4, p. 47 (see below), available at www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.

[22] Cybercrime Study, Chapter 7, p. 187.

[23] Cybercrime Study, Chapter 7, pp. 197-215.

tools offer a multifaceted combination of knowledge tools with regard to the collection and sharing of electronic evidence.

39. Although no UNODC tool has been exclusively devoted to electronic evidence, the following is an overview of UNODC guiding/research material/tools which are of relevance for the topic under discussion.

A. Studies by the United Nations Office on Drugs and Crime, prepared pursuant to United Nations resolutions

40. Pursuant to relevant mandates of the Economic and Social Council, the United Nations Office on Drugs and Crime has launched over the last years the following studies which touch upon, inter alia, the collection and sharing of electronic evidence in the context of specific crime types: (a) the Handbook on Identity-related Crime;[24] and (b) the Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children[25] (hereinafter referred to as "Study on the Abuse and Exploitation of Children").

41. Similarly, pursuant to General Assembly resolutions 65/230 and 67/189, UNODC provided secretarial and technical support to the meetings of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime. In this context, UNODC prepared, on the basis of the information provided by Member States a Draft Comprehensive Study on Cybercrime, which was cited as reference material in different parts of the present background paper.

1. Handbook on identity-related crime

42. Released by UNODC in 2011, pursuant to Economic and Social Council resolutions 2007/20 and 2009/22 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, the Handbook focuses on certain legal and policy issues pertaining to identity-related crime, including the gathering and use of electronic data and information. Its main objective is to lay out a range of options and considerations to be taken into account when addressing domestic criminal justice matters (typology of crimes/criminalization approaches/protection of victims), specific challenges in the field of international cooperation in criminal matters or the potential of synergies and partnerships between the public and the private sector, mainly in the area of prevention of identity-related crime. The combination of both research papers and practice-oriented material as segments of the Handbook serves the purpose of shedding light on different aspects and parameters of the complex problems posed by this form of crime.

43. Due to the diversity of the issues covered, the Handbook is destined for use by legislators, policymakers, prosecution and law enforcement authorities and practitioners, as well as other stakeholders (representatives from international and

---

[24] www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

[25] See footnote 21.

intergovernmental organizations active in this field, representatives from the private sector and experts from academia).

44. It can also be used as a resource material in technical assistance programmes and capacity-building activities with a view to increasing expert knowledge to address legal, institutional and operational issues around identity-related crime as an emerging form of crime.

45. In addition, the practical guide to international cooperation to combat identity-related crime, contained in the *Handbook on Identity-related Crime*, provides an overview of aspects pertaining to the transnational dimension of identity-related crime and focuses on basic information and guidelines on how to best deal with international cooperation requests in that field, including through relevant case examples.

2. Study on the effects of new information technologies on the abuse and exploitation of children

46. In response to Economic and Social Council resolution 2011/33, entitled "Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children", UNODC released in 2015 a Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children (initially presented at the 23rd session of the Commission on Crime Prevention and Criminal Justice in May 2014). The UNODC study was based on open source research on the issue as well as the work of a UNODC Informal Expert Group Meeting on the subject, which was convened in Vienna from 23 to 25 September 2013 and brought together experts from international organizations, law enforcement, other relevant practitioners and members of the academia. The Study provides relevant background information on the following issues:

(a) Emerging definitions and terms;

(b) The typology of the crimes;

(c) Most common types and forms of related behaviours;

(d) The main forms of information and communication technologies that facilitate certain crime types, such as child abuse and exploitation;

(e) The profile and technological sophistication of the offender;

(f) Victimization risk factors;

(g) The nature of the materials such as photographs, negatives, slides, magazines, books, drawings, movies, videotapes and computer disks or files; and

(h) The type of devices and platforms used for criminal purposes, such as: mobile phones, remote storage services that include built-in encryption technology, cloud computing and new applications such as Snap Chat and Wickr that enable users to distribute temporary images that disappear within seconds following receipt.

47. In addition, Chapter III of the Study is devoted to the investigation of ICT-facilitated child abuse and exploitation.

48. The study elaborates on the accessibility and practical application of image-related software and technologies that enable law enforcement agencies to identify and rescue unidentified victims seen in on line materials, as well as to triage their forensic investigations by comparing suspects' digital materials to images in databases. It provides useful information on innovating technologies used to reduce redundancy in investigative efforts, while serving the interests of victim-protection. They include, for instance:

Microsoft's "PhotoDNA": A free of charge software that is used to create a unique signature for a digital image, similar to a fingerprint, which can be compared with the signatures of other images to find copies of that image

Databases of abuse images that include information on identified and unidentified victims[26] and

INTERPOL's International Child Sexual Exploitation Image Database: A database that is used to identify and rescue previously unidentified victims, by using sophisticated image comparison software to make connections between victims and places.

49. The above-mentioned technical innovations are also used by Internet Service Providers to algorithmically find and remove child sexual abuse material from their servers.

50. Furthermore, digital forensics is described by the Study as a branch of forensic science concerned with the recovery and investigation of computer-generated digital traces. In this regard, the study sheds light on the type of computer data and electronic communications potentially relevant to a criminal act, the variety of possible formats and systems used to file it, as well as the tools employed to data examination.

51. The study also addresses the use of "automated search" software for forensic investigations. It underlines the use of this tool to easily and quickly find sites and content which are tagged with commonly used keywords.

52. The study further looks at the advances undertaken during the past decade on the development and deployment of technology tools and software that enable quick search of relevant data in thousands of distinct databases, financial records, DNA samples, sound samples, video clips, maps, floor plans, human intelligence reports and social networks. These tools weave together the relevant data into an accurate, coherent and useful trajectory, providing conceptual link analysis.

53. In addition, the study looks at the suitability and specificities of undercover work investigations with regard to online crime.

3. Draft comprehensive study on cybercrime

54. Chapter 6 of the draft comprehensive study on cybercrime elaborates on the topic of electronic evidence and criminal justice, starting from the need to identify, collect and analyse electronic evidence through digital forensics. It examines the

[26] Such as the databases developed by INTERPOL and the United States-based National Centre for Missing and Exploited Children (NCMEC).

admissibility and use of electronic evidence in criminal trials, and demonstrates how a range of prosecutorial challenges can impact on criminal justice system performance. It links law enforcement and criminal justice capacity needs with a view of delivered and required technical assistance activities.

55. In addition, certain aspects related to electronic evidence, are addressed from the scope of law enforcement and international cooperation. In this regard, Chapter 5 (Law enforcement and investigations) addresses the examination, used, storage, retention and preservation of electronic data that can be submitted as electronic evidence; real-time collection of data; remote forensic tools; direct law enforcement access to extraterritorial data; human rights and law enforcement investigations and obtaining data from private service providers. On the other hand, Chapter 7 (International cooperation) touches upon the issue of extraterritorial evidence from clouds and service providers elaborating on areas such as data location; access to extraterritorial data during evidence gathering; obtaining data from extraterritorial service providers.

B. Tools developed by the United Nations Office on Drugs and Crime for use in the context of technical assistance activities

56. The UNODC technical assistance programmes have led to the development of practical tools that address the topic of digital evidence from a practitioners' point of view. In this regard, participants of the Second Inter-regional meeting on Sharing Practices in Requesting and Providing Digital Evidence in Organized Crime Investigations and Prosecutions[27] formulated a set of basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions.

57. The set of basic tips provides practical advice for requesting electronic evidence from foreign jurisdictions, including, obtaining electronic evidence from open sources or directly from Internet Service Providers established or registered in the requesting country as affiliate companies of foreign-based ISP; preserve electronic evidence prior to sending the request for its disclosure; when possible, send the request directly to the ISP and send a copy of it to the investigative or prosecutorial body of the requested country; consult with cybercrime unit about the technical aspects of the request.

58. Pursuant to resolution 7/4 of the Conference of the Parties to the Organized Crime Convention, UNODC continues the development of tools for international cooperation, including the Mutual Legal Assistance Request Writer Tool (MLARWT). In this regard, UNODC has organized a number of informal expert group meetings to review and discuss the re-development of this tool and consider future directions regarding its use.

59. During the last informal expert group meeting in May 2015, participants agreed on the inclusion in the redeveloped tool of a digital evidence module that

---

[27] Tbilisi, Georgia, 9-11 December 2014. This tool was developed as part of the UNODC initiative to establish and reinforce the network of prosecutors and central authorities from Source, Transit and Destination Countries in response to Transnational Organized Crime in Central Asia and Southern Caucasus.

may assist States in requesting assistance related to this type of evidence. In this regard, experts shared national experience regarding requesting and obtaining digital evidence, including the extent to which templates for digital evidence are available and whether standardized approaches to describing digital evidence exist. The meeting provided guidance as to the possible format and structure of the digital evidence module, with a focus on different types of digital evidence, such as device data, network data, subscriber information and content data. The MLARWT, in its redeveloped version, was to be finalized as a result of a new informal expert group meeting convened from 22 to 23 October 2015 in Vienna.

C. Knowledge management platforms of the United Nations Office on Drugs and Crime

1. Sharing Electronic Resources and Laws on Crime (SHERLOC)

60. UNODC has continued to work on the development of SHERLOC, a knowledge management portal aimed at sharing legal resources on crime. SHERLOC has focused on compiling resources on different crime-types and related topics, among which, that of electronic evidence. As of 18 August 2015, it contains 44 relevant pieces of legislation setting standards on the matter of electronic evidence.

2. Cybercrime repository

61. In addition to SHERLOC, UNODC has created a Cyber Crime repository, which is a central database of laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.

62. Launched in 2015, the repository is the first available global tool containing laws, cases and lessons learned on cybercrime and electronic evidence, based on information provided and updated by Member States. The aim of the repository is multifaceted and includes: enabling lawmakers to draw upon the database of legislation when drafting laws on cybercrime or electronic evidence; facilitating international cooperation by helping law enforcement and prosecutors to identify cybercrime legislative provisions applicable in other Member States; and providing users with examples of good practices in the prevention, investigation and prosecution of cybercrime. Not all national legislation on mutual legal assistance refers to or sets out the functions of a central authority. Where it does, national legislation may designate a government institution as the central authority, provide a list of its functions and, in some cases, provide a saving clause confirming that the law does not limit the power of the authority to make or receive requests or to cooperate with a foreign State through other channels or means. By way of example, the legal assistance law of one European country specifies that the central authority shall “(1) receive requests for assistance …; (2) carry out, either directly or through [other] authorities, the execution of requests …; (3) transmit requests for assistance; as well as (4) carry out translations of documents”.

IV. Conclusions and recommendations

63. The Working Group on International Cooperation may wish to recommend that the Conference of the Parties:

(a) Request the Secretariat to prepare, in cooperation with relevant intergovernmental organizations, and subject to the availability of extrabudgetary funds, a manual on the collection and sharing of electronic evidence;

(b) Request the Secretariat, as part of its efforts to upgrade the tools on international cooperation, to mainstream the topic of electronic evidence;

(c) Request Member States to notify the Secretariat of the existence of specialized cybercrime units or structures, for inclusion in the CNA directory.