United Nations E/CN.15/2011/19

Economic and Social Council

Distr.: General
2 March 2011

Original: English

Commission on Crime Prevention and Criminal Justice
Twentieth session
Vienna, 11-15 April 2011
Item 6 of the provisional agenda*
World crime trends and emerging issues and responses in the field of crime prevention and criminal justice

Report of the open-ended intergovernmental expert group on the comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector

Note by the Secretariat

1. Pursuant to paragraph 9 of General Assembly resolution 65/230, the open-ended intergovernmental expert group established by the Commission in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World (General Assembly resolution 65/230, annex) held its meeting in Vienna from 17 to 21 January 2011. In accordance with its mandate, the expert group deliberated on the question of

> a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

2. In paragraph 11 of resolution 65/230, the General Assembly requested the open-ended intergovernmental expert group to report to the Commission on progress in its work. Accordingly, the expert group reviewed and adopted the annexed outcome documents, entitled "Collection of topics for consideration in a comprehensive study on impact of and response to cybercrime" (annex I) and

* E/CN.15/2011/1.

"Methodology for the study" (annex II), transmitted to the Commission at its twentieth session for its consideration.

3. Following the adoption of the collection of topics for consideration within a comprehensive study on impact of and response to cybercrime (annex I), the representative of Colombia made the following statement and requested that it be included in the report of the open-ended intergovernmental expert group:

> 1. During the meeting of the open-ended intergovernmental expert group, many delegations expressed their concerns about the frequent misuse of new information and communications technologies for terrorist purposes. In this context, a representative of the Secretariat made a presentation about the work of the United Nations Office on Drugs and Crime on this problem and, in particular, the misuse of the Internet. Taking into account that the study of cybercrime must be full and comprehensive, it would need to address all of the concerns expressed. This makes it critical that all aspects of the relationships between terrorism and cybercrime should be included in the study. Terrorist organizations use these technologies in a range of different ways, such as:
>
> (a) For propaganda purposes;
>
> (b) To gather information;
>
> (c) As a training tool;
>
> (d) To organize illicit activities;
>
> (e) To disseminate information for purposes of recruitment and incitement;
>
> (f) For purposes of secure storage and transmission of information;
>
> (g) To attack computer networks themselves.
>
> 2. In the interests of consensus, Colombia accepts the proposals of the delegation of Argentina concerning this subject matter, but requests that in the report of the open-ended intergovernmental expert group on its first meeting, note be taken of the following:
>
> (a) With respect to paragraph 12 of the collection of topics for consideration within a comprehensive study on impact of and responses to cybercrime (see annex I), Colombia understands that the reference to an inventory of conduct that has been criminalized includes the subject matter of terrorism;
>
> (b) With respect to the title preceding paragraph 18 of that document, Colombia understands that the challenges of cybercrime also include the subject matter of terrorism;
>
> (c) Colombia also expresses the hope that the study will include consideration of the possible misuse by terrorists of tools that can be used to commit cybercrime, as mentioned in paragraph 25 of that document.

Annex I

Collection of topics for consideration within a comprehensive study on impact of and response to cybercrime

I. Introduction

1. During the Twelfth United Nations Congress on Crime Prevention and Criminal Justice in 2010, member States discussed in some depth the issue of cybercrime and decided to invite the Commission on Crime Prevention and Criminal Justice to convene an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, as well as the response to it. That recommendation was adopted by the Commission on Crime Prevention and Criminal Justice and then by the Economic and Social Council in its resolution 2010/18 and by the General Assembly in its resolution 65/230.

2. In line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, the comprehensive study is to examine:

> the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

3. Paragraph 42 of the Salvador Declaration thus identifies the various substantive aspects that the study should investigate (the problem of cybercrime, national legislation, best practices, technical assistance and international cooperation), and also the perspective (the response by Member States, the international community and the private sector) and the focus (examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime).

4. In order to draft a structure for the study, these three dimensions (substantive aspects, perspective and focus) have been converted into 12 topics that follow the mandate of the Declaration. The 12 topics are grouped below in categories.

Problem of cybercrime (topics 1-3)

5. The Salvador Declaration highlights that the study should investigate the problem of cybercrime. In order to address the full extent of problems posed by cybercrime, three key areas are identified for detailed analysis:

(a) Phenomenon of cybercrime (topic 1);

(b) Statistical information (topic 2);

(c) Challenges of cybercrime (topic 3).

Legal responses to cybercrime (topics 4-9)

6. The Salvador Declaration calls for a study of legal responses to cybercrime including the exchange of information on national legislation, best practices and international cooperation. In addition to general aspects of harmonization of legislation, specific areas of legal responses are identified:

(a) Common approaches to legislation (topic 4);

(b) Criminalization (topic 5);

(c) Procedural powers (topic 6);

(d) International cooperation (topic 7);

(e) Safeguards and conditions, including protection of fundamental human rights and personal data;

(f) Respect for the principle of sovereign equality of States and non-interference in the affairs of other States;

(g) Electronic evidence (topic 8);

(h) Roles and responsibilities of service providers and the private sector (topic 9).

Crime prevention and criminal justice capabilities and other responses to cybercrime (topic 10)

7. The Salvador Declaration refers not only to the study of legal responses to cybercrime, but also more broadly to other types of responses to cybercrime.

International organizations (topic 11)

8. The Salvador Declaration calls for an analysis of responses by Member States, the international community and the private sector. While matters relating to the legal responses undertaken by the international community are covered under the heading of legal responses, a separate heading for responses of the international community will facilitate the analysis of more general aspects, such as the relation between regional and international approaches.

Technical assistance (topic 12)

9. Given the impact of cybercrime on developing countries and the need for a uniform and coordinated approach to combating cybercrime, technical assistance is addressed as one specific area to be covered by the comprehensive study.

II. Detailed overview of topics

Topic 1. Phenomenon of cybercrime

Background

10. Computer crime and, more specifically, cybercrime are terms used to describe a specific category of criminal conduct. The challenges related to this category of

criminal conduct include both the wide range of offences covered and also the dynamic development of new methods of committing crimes.

The development of computer crime and cybercrime

11. In the 1960s, when transistor-based computer systems were introduced and computers became more popular,[1] criminalization of offences focused on physical damage to computer systems and stored data.[2] The 1970s were characterized by a shift from traditional property crimes against computer systems[3] to new forms of crime[4] that included the illegal use of computer systems[5] and the manipulation[6] of electronic data.[7] The shift from manual to computer-operated transactions led to another new form of crime: computer-related fraud.[8] In the 1980s, personal computers became more and more popular, and for the first time a broad range of critical infrastructure became dependent on computer technology.[9] One of the side effects of the distribution of computer systems was an increasing interest in software, and the first forms of software piracy and crimes related to patents began to appear.[10] In addition, the beginning of the interconnection of computer systems enabled offenders to enter a computer system without being present at the crime scene.[11] The introduction of the graphical interface (World Wide Web) in the 1990s, which was followed by rapid growth in the number of Internet users, led to new

[1] Regarding the related challenges see R. T. Slivka and J. W. Darrow, "Methods and problems in computer security", *Rutgers Journal of Computers and the Law*, vol. 5, No. 2 (1976), pp. 217-269.

[2] McLaughlin, "Computer crime: the Ribicoff Amendment to United States Code, Title 18", *Criminal Justice Journal*, vol. 2, 1978, pp. 217 ff.

[3] Gemignani, "Computer crime: the law in '80", *Indiana Law Review*, vol. 13, 1980, p. 681.

[4] McLaughlin, "Computer crime: the Ribicoff Amendment".

[5] Freed, *Materials and Cases on Computer and Law* (n.p., 1971), p. 65.

[6] Bequai, "The electronic criminals: how and why computer crime pays", *Barrister*, vol. 4, 1977, pp. 8 ff.

[7] *Criminological Aspects of Economic Crime: Proceedings of the 12th European Conference of Directors of Criminological Research Institutes (November 1976)*, vol. XV, Collected Studies in Criminological Research (Strasbourg, Council of Europe, 1977), pp. 225 ff.; United States of America, *Staff Study of Computer Security in Federal Programs: Committee on Government Operations — United States Senate* (Washington, D.C., United States Government Printing Office, 1977).

[8] McLaughlin, "Computer crime: the Ribicoff Amendment" (see footnote 2 above); Bequai, "Computer crime: a growing and serious problem", *Police Law Quarterly*, vol. 6, 1977, p. 22.

[9] E. A. Glynn, "Computer abuse: the emerging crime and the need for legislation", *Fordham Urban Law Journal*, vol. 12, No. 1 (1983-1984), p. 73.

[10] BloomBecker, "The trial of computer crime", *Jurimetrics Journal*, vol. 21, 1981, p. 428; W. Schmidt, "Legal proprietary interests in computer programs: the American experience", *Jurimetrics Journal*, vol. 21, 1981, pp. 345 ff.; M. Dunning, "Some aspects of theft of computer software", *Auckland University Law Review*, vol. 4, No. 3 (1982), pp. 273 ff.; Weiss, "Pirates and prizes: the difficulties of protecting computer software", *Western State University Law Review*, vol. 11, 1983, pp. 1 ff.; R. P. Bigelow, "The challenge of computer law", *Western England Law Review*, vol. 7, No. 3 (1985), p. 401; G. Thackeray, "Computer-related crimes: an outline", *Jurimetrics Journal*, vol. 25, No. 3 (1985), pp. 300 ff.

[11] Yee, "Juvenile computer crime: hacking — criminal and civil liability", *Comm/Ent Law Journal*, vol. 7, 1984, pp. 336 ff.; "Who is calling your computer next? Hacker!", *Criminal Justice Journal*, vol. 8, 1985, pp. 89 ff.; A. M. Wagner, "The challenge of computer-crime legislation: how should New York respond?", *Buffalo Law Review*, vol. 33, No. 3 (1984), pp. 777 ff.

methods of criminal conduct. The distribution of child abuse material, for example, moved from the physical exchange of books and tapes to online distribution through websites and Internet services.[12] Although computer crimes were generally local crimes, the Internet turned electronic crime into transnational crime. The first decade of the twenty-first century was dominated by new, very sophisticated methods of committing crimes, such as “phishing”,[13] “botnet”[14] attacks, and emerging uses of technology such as voice-over-Internet protocol (VoIP) communication[15] and “cloud computing”,[16] which create difficulties for law enforcement.

Scope of the study

12. The study on this topic will focus on the phenomenon of cybercrime itself and does not include responses to cybercrime:

(a) Analysis of the phenomenon of cybercrime by taking into account those acts that are covered by existing legal frameworks;

(b) Inventory of offences that are criminalized;

(c) Inventory of conduct that is not yet criminalized;

(d) Overview of combined offences (such as “phishing”) and future trends;

(e) Inventory of relevant cases;

(f) Examination of the importance of the definition of cybercrime.

[12] “Child pornography”, theme paper prepared for the Second World Congress against Commercial Sexual Exploitation of Children, Yokohama, Japan, 12-20 December 2001, p. 17; “Sexual exploitation of children over the Internet”, report prepared for the use of the Committee on Energy and Commerce, United States, House of Representatives, 109th Congress, January 2007, p. 9.

[13] The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. The term “phishing” originally described the use of e-mails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” is linked to popular hacker naming conventions. For more information see International Telecommunications Union, *Understanding Cybercrime: A Guide for Developing Countries* (Geneva, 2009), chap. 2.8.4.

[14] Botnets is a short term for a group of compromised computers running software under external control. For more details, see Clay Wilson, “Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress”, Congressional Research Service Report RL32114, 2007, p. 4.

[15] M. Simon and J. Slay, “Voice over IP: forensic computing implications”, paper prepared for the fourth Australian Digital Forensics Conference, Perth, 4 December 2006.

[16] Cristos Velasco San Martin, “Jurisdictional aspects of cloud computing”, paper presented at the Council of Europe Octopus Interface Conference: Cooperation against Cybercrime, Strasbourg, 10-11 March 2009; M. Gercke, “Die Auswirkungen von Cloud Storage auf die Tätigkeit der Strafverfolgungsbehörden”, in *Inside the Cloud: Neue Herausforderungen für das Informationsrecht*, J. Taeger and A. Wiebe, eds., Oldenburger Tagungsbände (Edewecht, Germany, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2009), pp. 499 ff.

Topic 2. Statistical information

Background

13. Crime statistics provide the basis for discussion and decision-making by policymakers and academics.[17] Furthermore, access to precise information about the true extent of cybercrime can enable law enforcement agencies to improve anti-cybercrime strategies, deter potential attacks and ensure that more appropriate and effective legislation is enacted.

Current status of crime statistics on cybercrime

14. Information about the extent of crime is generally taken from crime statistics and surveys.[18] The use of both types of sources presents challenges when used to develop policy recommendations. First of all, crime statistics are generally created at the national level and do not reflect the international extent of the matter. While it would theoretically be possible to combine the data between different States, this approach would not produce reliable information because of differences in legislation and recording practice.[19] Combining and comparing national crime statistics requires a certain degree of compatibility[20] that is lacking when it comes to cybercrime. Even if cybercrime offences are recorded, they are not necessarily listed separately.[21]

15. Secondly, statistics can reflect only crimes that have been detected and reported.[22] Especially with regard to cybercrime, there are concerns that the number of unreported cases appears to be significant.[23] Businesses may fear that negative

[17] P. A. Collier and B. J. Spaul, “Problems in policing computer crime”, *Policing and Society*, vol. 2, No. 4 (1992), p. 308.

[18] Regarding the emerging importance of crimes statistics see D. A. Osborne and S. C. Wernicke, *Introduction to Crime Analysis: Basic Resources for Criminal Justice Practice* (Binghamton, New York, Haworth Press, 2003), pp. 1 ff.

[19] See in this context: *Overcoming Barriers to Trust in Crimes Statistics: England and Wales*, Monitoring Report No. 5, interim report (London, United Kingdom Statistics Authority, December 2009), p. 9. Available from www.statisticsauthority.gov.uk.

[20] A. Alvazzi del Frate, “Crime and criminal justice statistics challenges”, in *International Statistics on Crime and Justice*, S. Harrendorf, M. Heiskanen and S. Malby, eds., HEUNI Publication Series, No. 64 (Helsinki, European Institute for Crime Prevention and Control, affiliated with the United Nations, 2010), p. 168. Available from www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

[21] “Computer crime”, Parliamentary Office of Science and Technology, *Postnote*, No. 271, October 2006, p. 3.

[22] Regarding the related challenges see M. E. Kabay, “Understanding studies and surveys of computer crime”, June 2009. Available from www.mekabay.com/methodology/crime_stats_methods.pdf.

[23] “The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company information technology systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. “It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack,” explained Mark Mershon, acting head of the FBI New York office. See “FBI wants to know more about hacker attacks”, *Heise News*, 27 October 2006. Available from www.h-online.com/security/news/item/FBI-wants-to-know-more-about-hacker-attacks-731717.html. See also “Comments on computer crime: Senate

publicity could damage their reputation.[24] If a company announces that hackers have accessed its server, customers may lose faith, resulting in costs that could be greater than the losses caused by the hacking attack. If, however, offences are not reported and prosecuted, the offenders may go on to reoffend. Victims may not believe that law enforcement agencies will be able to identify offenders[25] and may see little point in reporting offences.[26] Since the automation of cybercrime attacks enables cybercriminals to develop a strategy of reaping large profits from many attacks targeting small amounts (which happens with advance fee fraud cases),[27] the possible impact on unreported crimes could be significant. Where they have lost only small amounts, victims may prefer not to go through with time-consuming procedures of reporting to law enforcement. In practice, those cases that are reported often involve extremely high fees.[28]

Scope of the study

16. The study on this topic will consist of the following:

(a) Collection of the most recent statistics, surveys and analyses addressing the prevalence and extent of cybercrime;

(b) Evaluation of the value of statistics for policy recommendations;

(c) Determination of possible obstacles in the collection of accurate statistics;

(d) Identification of countries that specifically gather statistics on cybercrime offences;

(e) Evaluation of need for and advantages of collecting statistical information on cybercrime;

Bill S. 240", *Memphis State University Law Review*, 1980, p. 660.

[24] See N. Mitchison and R. Urry, "Crime and abuse in e-business", in *IPTS Report*, No. 57, 2001, pp. 18-22; Collier and Spaul, "Problems in policing computer crime" (see footnote 17 above), p. 310.

[25] See Collier and Spaul, "Problems in policing computer crime" (see footnote 17 above), p. 310; R. G. Smith, "Investigating cybercrime: barriers and solutions", paper prepared for the Association of Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney, 11 September 2003, p. 2. Available from www.aic.gov.au/about_aic/research_programs/staff/smith_russell.aspx.

[26] In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see "Interpol in appeal to find paedophile suspect", *New York Times*, 9 October 2007. Available from www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the International Criminal Police Organization (INTERPOL) website, available from www.interpol.int/Public/THB/vico/Default.asp.

[27] See United Kingdom, Serious Organised Crime Agency, "International crackdown on mass marketing fraud revealed", 2007.

[28] In the *2006 NW3C Internet Crime Report*, published by the National White Collar Crime Center, only 1.7 per cent of the reported total United States dollar losses were related to the Nigerian letter fraud, but those cases that were reported had an average loss of $5,100 each. The number of reported offences is very low, while the average loss of those offences is high.

(f) Examination of possible techniques that could be used to collect such information;

(g) Discussion of a possible model of a central authority hosting statistical information.

Topic 3. Challenges of cybercrime

Background

17. Much attention is currently being paid to the development of strategies to address the specific challenges of cybercrime. The reasons for this development are twofold: first, that some of the instruments required to investigate cybercrime are new and therefore require intensive research, and second, that investigating crimes involving network technology is accompanied by several unique challenges not encountered in traditional investigations.

Challenges of fighting cybercrime and related threats

18. The list of unique technical and legal challenges of cybercrime is long. The fact that offenders can commit cybercrimes by using devices that do not require in-depth technical knowledge, such as software tools[29] designed to locate open ports or break password protection, is just one example.[30] Another challenge is the difficulty of tracing offenders. Although users leave multiple traces while using Internet services, offenders can hinder investigations by disguising their identity. If, for example, offenders commit offences by using public Internet terminals or open wireless networks, it can be difficult to identify them. A more general challenge in investigating cybercrime arises from the fact that, from a technological point of view, the Internet offers few control instruments that can be used by law enforcement. The Internet was originally designed as a military network[31] based on a decentralized network architecture that sought to keep its main functionality intact even when components of the network were attacked. This decentralized approach was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network, and investigative measures that require a means of control pose unique challenges in this environment.[32]

[29] "Websense", *Security Trends Report 2004*, p. 11; United States of America, General Accounting Office, *Information Security: Computer Controls over Key Treasury Internet Payment System*, GAO-03-837 (Washington, D.C., 2003), p. 3; U. Sieber, "The threat of cybercrime", in *Organised Crime in Europe: The Threat of Cybercrime — Situation Report 2004* (Strasbourg, Council of Europe Publishing, 2005), p. 143.

[30] K. Ealy, "A new evolution in hack attacks: a general overview of types, methods, tools, and prevention", SANS Institute, 2003, p. 9.

[31] For a brief history of the Internet, including its military origins, see B. Leiner and others, "A brief history of the Internet", available from www.isoc.org/internet/history/brief.shtml.

[32] H. F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Pittsburgh, Carnegie Mellon University, Software Engineering Institute, 2002).

Scope of the study

19. The study on this topic will consist of the following:

(a) Comprehensive inventory of challenges related to the fight against cybercrime;

(b) Summary of best practices, both technical and legal, in addressing those challenges.

Topic 4. Common approaches to legislation

Background

20. In the last 20 years, various countries and regional organizations have developed legislation and legal frameworks to address cybercrime. Despite certain common trends that have developed, the differences in national legislation remain significant.

National and regional differences

21. One reason for both national and regional differences in legislative frameworks is that the impact of cybercrime is not universally the same, as the fight against spam demonstrates.[33] Spam has emerged as a much more serious issue in developing countries than in Western countries as a result of the scarcity and expense of resources.[34] In terms of illegal content, some countries and regions may criminalize the dissemination of material that may be considered to be protected by the principle of freedom of speech[35] in others.[36]

[33] *Understanding Cybercrime: A Guide for Developing Countries* (see footnote 13 above), chap. 2.6.7.

[34] See Organization for Economic Cooperation and Development, “Spam issues in developing countries”, document DSTI/CP/ICCP/SPAM(2005)6/FINAL, 26 May 2005, p. 4. Available from: www.oecd.org/dataoecd/5/47/34935342.pdf.

[35] Regarding the principle of freedom of speech see T. L. Tedford and D. A. Herbeck, *Freedom of Speech in the United States*, 5th ed. (State College, Pennsylvania, Strata, 2005); E. Barendt, *Freedom of Speech* (Oxford, Oxford University Press, 2007); C. E. Baker; *Human Liberty and Freedom of Speech* (New York, Oxford University Press, 1989); J. W. Emord, *Freedom, Technology and the First Amendment* (San Francisco, Pacific Research Institute for Public Policy, 1991); regarding the importance of the principle with regard to electronic surveillance see C. Woo and M. So, “The case for Magic Lantern: September 11 Highlights — the need for increasing surveillance”, *Harvard Journal of Law and Technology*, vol. 15, No. 2 (2002), pp. 530 ff.; M. Chesterman, *Freedom of Speech in Australian Law: A Delicate Plant* (Aldershot, Hampshire, Ashgate, 2000); E. Volokh, “Freedom of speech, religious harassment law, and religious accommodation law”, *Loyola University Chicago Law Journal*, vol. 33, 2001, pp. 57 ff., available from www.law.ucla.edu/volokh/harass/religion.pdf; H. Cohen, “Freedom of speech and press: exceptions to the First Amendment”, Congressional Research Service Report 95-815, 2009, available from www.fas.org/sgp/crs/misc/95-815.pdf.

[36] Concerns over freedom of expression (e.g. the First Amendment to the United States Constitution) explain why certain acts of racism were not made illegal by the Convention on Cybercrime (Council of Europe, *European Treaty Series*, No. 185), but their criminalization was included in the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer

22. As cybercrime is a truly transnational crime,[37] international cooperation is an essential requirement for successful investigations and prosecutions.[38] Effective international cooperation requires a degree of common understanding and the adoption of common approaches of legislation in order to prevent the establishment of safe havens.[39]

23. The study on this topic will consist of the following:

(a) Analysis of efforts to adopt common approaches to cybercrime legislation;

(b) Other elements with regard to the adoption of common approaches of cybercrime legislation, including the perceived seriousness of the conduct and the impact of human rights norms;

(c) Compilation of an inventory of how countries implement legal standards from regional organizations and an analysis to determine which techniques can help to ensure consistency in the approaches;

(d) Analysis of the extent to which differences in cybercrime legislation affect international cooperation.

Topic 5. Criminalization

Background

24. The effective investigation and prosecution of cybercrime will require the establishment of new offences if certain conduct is not already covered by existing legislation. The existence of adequate legislation is not only relevant for national investigations, but can also have an impact on international cooperation, as outlined above.

Systems (Council of Europe, *European Treaty Series*, No. 189). See also the explanatory report to the Additional Protocol, available from http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[37] Regarding the extent of transnational attacks in the most damaging cyber attacks see A. D. Sofaer and S. E. Goodman, "Cyber crime and security: the transnational dimension", in *The Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), p. 7. Available from http://media.hoover.org/documents/0817999825_1.pdf.

[38] Regarding the need for international cooperation in the fight against cybercrime see T. L. Putnam and D. D. Elliott, "International responses to cyber crime", in *Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), pp. 35 ff., available from http://media.hoover.org/documents/0817999825_35.pdf; and Sofaer and Goodman, "Cyber crime and security: the transnational dimension".

[39] Regarding the dual criminality principle in international investigations see "United Nations Manual on the Prevention and Control of Computer-Related Crime", *International Review of Criminal Policy*, Nos. 43 and 44, 1994 (United Nations publication, Sales No. E.94.IV.5), para. 269, available from www.uncjin.org/Documents/EighthCongress.html; Judge Stein Schjolberg and Amanda M. Hubbard, "Harmonizing national legal approaches on cybercrime", paper prepared for the International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June-1 July 2005, p. 5.

Substantive criminal law

25. Most comprehensive regional frameworks set up to address cybercrime contain a set of substantive criminal law provisions that are designed to close gaps in national legislation. Standard provisions in these frameworks include the criminalization of illegal access, illegal interception, illegal data interference, illegal system interference, computer-related fraud and computer-related forgery. Some national frameworks could go further and criminalize offences such as the production and distribution of tools (such as software or hardware) that can be used to commit cybercrime, or for terrorist purposes, acts related to child abuse material, grooming or hate speech.

Scope of the study

26. The study will build upon the findings of the study on topic 1, on the phenomenon of cybercrime:

(a) Inventory of national and regional approaches to the criminalization of cybercrime, including in relation to participation and attempt;

(b) Evaluation of best practices in regard to criminalization;

(c) Analysis of differences in the approach of different legal systems and traditions to the criminalization of cybercrime.

Topic 6. Procedural powers

Background

27. In order to carry out effective investigations, law enforcement agencies need to have access to investigative procedures that enable them to take the measures necessary to identify the offender and collect the evidence required for criminal proceedings.[40] These measures may be the same as those used in traditional investigations not related to cybercrime. However, given that the offender does not necessarily need to be present at or even near the crime scene, it is very likely that cybercrime investigations will need to be conducted in a different way from traditional investigations.[41]

[40] Regarding user-based approaches in the fight against cybercrime see S. Görling, “The myth of user education”, paper prepared for the Virus Bulletin Conference, Montreal, 11-13 October 2006, available from www.virusbtn.com/conference/vb2006/abstracts/Gorling.xml. See also the comment made by Jean-Pierre Chevènement, French Minister of the Interior, at a Group of Eight conference on security and trust in cyberspace in Paris in 2000: “More broadly, we have to educate users. They must all understand what they can and can’t do on the Internet and be warned of the potential dangers. As use of the Internet grows, we’ll naturally have to step up our efforts in this respect.”

[41] Due to the protocols used in Internet communication and the worldwide accessibility there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence see *Understanding Cybercrime: A Guide for Developing Countries* (see footnote 13 above), chap. 3.2.7.

Investigative measures

28. In addition to provisions relating to substantive cybercrime offences, most comprehensive regional frameworks set up to address cybercrime also contain a set of provisions specifically designed to facilitate cybercrime investigations. Standard provisions include specific search and seizure procedures, the expedited preservation of computer data, the disclosure of stored data, the interception of content data and the collection of traffic data.

29. Currently, law enforcement agencies are confronted with newly developed technologies that have a negative impact on classical investigation methods. Many of these challenges remain unaddressed.

Scope of the study

30. The study on this topic will consist of the following:

(a) Inventory of case examples of investigations that have highlighted the need for specific cybercrime investigative measures;

(b) Inventory of different investigative provisions contained in regional and national legal frameworks;

(c) Overview of the current needs of law enforcement agencies for specific investigative provisions relating to cybercrime to deal with the challenges created by new technologies;

(d) Analysis of differences in the approach to investigative provisions relating to cybercrime in different legal systems and traditions.

Topic 7. International cooperation

Background

31. An increasing number of cybercrimes have an international dimension,[42] particularly owing to the fact that offenders, operating through the transnational Internet, often do not need to be present at the location of the victim. This separation between the locations of the victim and the offender and the mobility of offenders make it necessary for law enforcement and judicial authorities to cooperate internationally and assist the State that has assumed jurisdiction.[43] Effective international cooperation poses one of the major challenges in combating increasingly globalized crime, both in its traditional forms and as cybercrime. Differences in legislation and practice among States can make international cooperation difficult, as can the relatively limited number of treaties and agreements

[42] Regarding the transnational dimension of cybercrime see Mike Keyser, "The Council of Europe Convention on Cybercrime", *Journal of Transnational Law and Policy*, vol. 12, No. 2 (2003), p. 289, available from www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. Sofaer and Goodman, "Cyber crime and security: the transnational dimension" (see footnote 37 above), pp. 1 ff.

[43] See in this context: *Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (United Nations publication, Sales No. E.05.V.2), p. 217. Available from www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

on international cooperation available to States.[44] Furthermore, the question of what should be considered an international matter in cybercrime cases should be discussed and agreed upon.

Instruments for international cooperation

32. There are different sources of the legal basis necessary for formal international cooperation such as extradition, mutual legal assistance in criminal matters and cooperation for the purposes of confiscation. Provisions on international cooperation may form a part of international and regional agreements, including the United Nations Convention against Transnational Organized Crime.[45]

Scope of the study

33. The study on this topic will consist of the following:

(a) Inventory of domestic legal approaches to the definition of an international matter in criminal law enforcement on the Internet;

(b) Examining options with regard to effective legal bases, including universal international bases, and other responses for combating cybercrime;

(c) Challenges to effective international cooperation, in particular extradition and mutual legal assistance, in cybercrime cases, including the application of dual criminality and differences in investigative measures;

(d) Inventory of national and international provisions dealing with international cooperation that are relevant for cybercrime investigations and prosecutions;

(e) Inventory of best-practice examples from bilateral and multilateral treaties and arrangements, inter alia, lessons learned from the functioning of the 24/7 network of focal points;

(f) Inventory of cybercrime cases involving international cooperation;

(g) Role of and challenges in relation to informal means of international cooperation such as information-sharing;

(h) Overview of the current needs of relevant authorities with regard to international cooperation;

(i) Identification of ongoing and ideas for future training programmes, exchanges of experiences, capacity-building and technical assistance activities to strengthen criminal justice capabilities and enable countries to cooperate internationally.

[44] Carlos A. Gabuardi, “Institutional framework for international judicial cooperation: opportunities and challenges for North America”, *Mexican Law Review*, vol. 1, No. 2 (2009), p. 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[45] United Nations, *Treaty Series*, vol. 2225, No. 39574; regarding the Convention see Jennifer M. Smith, “An international hit job: prosecuting organized crime acts as crimes against humanity”, *Georgetown Law Journal*, vol. 97, 2009, p. 1,118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

Topic 8. Electronic evidence

Background

34. As more and more information is kept in digital form, electronic evidence is relevant to both cybercrime investigations and traditional investigations. Computer and network technology have become a part of everyday life in developed countries and are increasingly becoming so in developing countries as well. The increasing capacity of hard drives[46] and the relatively low cost[47] of the storage of digital documents as compared to the storage of physical documents have led to a growing number of digital documents.[48] Today, a significant amount of data is stored only in digital form.[49] As a consequence of this increase, electronic documents such as text documents, digital videos and digital pictures[50] are playing a role in cybercrime investigations and related court proceedings.[51]

Rules for electronic evidence

35. Electronic evidence presents a number of challenges, at both the stage of its collection and that of its admission as evidence.[52] During the process of evidence collection, investigators must satisfy certain procedures and requirements, such as the special treatment required for the protection of the integrity of data. Law enforcement agencies require specific measures in order to carry out successful investigations. The availability of such measures is especially relevant if traditional

[46] See D. Abramovitch, "A brief history of hard drive control", *IEEE Control Systems Magazine*, vol. 22, No. 3 (2002), pp. 28 ff.; T. Coughlin, D. Waid and J. Porter, "The disk drive: 50 years of progress and technology innovation — the road to two billion drives", *Computer Technology Review*, April 2005, available from www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[47] S. M. Giordano, "Electronic evidence and the law", *Information Systems Frontiers*, vol. 6, No. 2 (2006), p. 161; S. D. Willinger and R. M. Wilson, "Negotiating the minefields of electronic discovery", *Richmond Journal of Law and Technology*, vol. 10, No. 5 (2004).

[48] Lange/Minster, Electronic Evidence and Discovery, p. 6.

[49] Chet Hosmer, "Proving the integrity of digital evidence with time", *International Journal of Digital Evidence*, vol. 1, No. 1 (2002), p. 1, available from www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[50] Regarding the admissibility and reliability of digital images see Jill Witkowski, "Can juries really believe what they see? New foundational requirements for the authentication of digital images", *Washington University Journal of Law and Policy*, vol. 10, 2002, pp. 267 ff.

[51] Michael Harrington, "A methodology for digital forensics", *Thomas M. Cooley Journal of Practical and Clinical Law*, vol. 7, 2004, pp. 71 ff.; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 2nd ed. (London, Academic Press, 2004), p. 14. Regarding the legal frameworks in different countries see C. A. Rohrmann and J.S.A. Neto, "Digital evidence in Brazil", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008; M. Wang, "Electronic evidence in China", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008; P. Bazin, "An outline of the French Law on digital evidence", *Digital Evidence and Electronic Signature Law Review*, No. 5, 2008; A. B. Makulilo, "Admissibility of computer evidence in Tanzania", *Digital Evidence and Electronic Signature Law Review*, No. 4, 2007; R. Winick, "Search and seizures of computers and computer data", *Harvard Journal of Law and Technology*, vol. 8, No. 1 (1994), p. 76; F. Insa, "Situation report on the admissibility of electronic evidence in Europe", in *Syllabus to the European Certificate on Cybercrime and E-Evidence*, 2008, p. 213.

[52] Casey, *Digital Evidence and Computer Crime* (see footnote 51), p. 9.

forms of evidence such as fingerprints or witness identification are not available. In those cases, the ability to successfully identify and prosecute an offender is based on the correct collection and evaluation of the digital evidence.[53]

36. Digitalization also influences the way in which law enforcement agencies and courts deal with evidence.[54] Whereas traditional documents are simply handed out in court, digital evidence may require specific procedures that are not suitable for conversion into traditional evidence, e.g. printouts of files.[55]

Scope of the study

37. The study on this topic will consist of the following:

(a) Inventory of provisions, safeguards and standards dealing with the collection, preservation, storage, analysis and admissibility of electronic evidence;

(b) Analysis of differences in the approach and the identification of common principles in relation to electronic evidence in different legal systems and traditions;

(c) Collection of best practices on specialized training, capacity-building and exchange of technology;

(d) Analysis on the mechanism of cross-border digital evidence exchange.

Topic 9. Roles and responsibilities of service providers and the private sector

Background

38. The prevention and investigation of cybercrime depends on a number of different elements. Even if the offender acted alone, the commission of a cybercrime automatically involves a number of people and businesses. Owing to the structure of the Internet, the transmission of a simple e-mail message requires the service of a number of providers: the e-mail provider, access providers and the routers who forward the e-mail message to the recipient. The situation is similar with regard to the downloading of material featuring child abuse. The downloading process involves the content provider who uploaded the pictures (for example, on a website), the hosting provider who provided the storage media for the website, the routers who forwarded the files to the user and finally the access provider who enabled the user to access the Internet.

[53] Regarding the need for a formalization of computer forensics see R. Leigland and A. W. Krings, “A formalization of digital forensics”, *International Journal of Digital Evidence*, vol. 3, No. 2 (2004).

[54] Regarding the difficulties of dealing with digital evidence on the basis of the traditional procedures and doctrines see R. Moore, “To view or not to view: examining the plain view doctrine and digital evidence”, *American Journal of Criminal Justice*, vol. 29, No. 1 (2004), pp. 57 ff.

[55] See John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed. (Hingham, Massachusetts, Charles River Media, 2005), p. 3. Regarding the early discussion about the use of printouts see Robinson, “The admissibility of computer printouts under the business records exception in Texas”, *South Texas Law Journal*, vol. 12, 1970, pp. 291 ff.

39. While emphasis is often placed on ensuring adequate legislation, private industry continues to play an important role in both preventing cybercrime and assisting in investigating it. Its involvement in cybercrime investigations is, however, accompanied by a number of challenges.

Legal issues

40. The fact that cybercrime cannot be committed without the involvement of the providers, coupled with the fact that providers often do not have the ability to prevent the commission of cybercrimes, raises the question of whether the responsibility of service providers should be limited. The answer to the question is critical for the economic development of the information and communications technology infrastructure.

41. The efforts of law enforcement agencies very often depend on the cooperation of Internet providers. This raises some concerns, as imposing or limiting the liability of service providers for acts committed by their users could have an impact on the cooperation and support of the service providers for cybercrime investigations, as well as on the actual prevention of cybercrime.

Role of industry

42. The role of industry in addressing cybercrime is complex; it may range from developing and implementing solutions to protect its own services from criminal abuse to user protection and the support of investigations. Self-protection measures adopted by an industry are often a logical component of comprehensive business strategies and generally do not require a specific legal basis as long as the measures do not involve illegal active countermeasures. Protection measures undertaken on behalf of users, provided they are undertaken with the consent of the user, are equally unproblematic. The involvement of the industry in criminal investigations, however, has presented challenges in many countries, and different approaches have been adopted. Some countries involve industry in criminal investigations purely on a voluntary basis and have developed guidelines to facilitate the cooperation of industry and law enforcement. Other countries have adopted a different approach, in which they have imposed legal obligations on industry to cooperate with law enforcement in criminal investigations.

Scope of the study

43. The study on this topic will consist of the following:

(a) Approaches and practices concerning the responsibility of service providers, including differentiating between the different types of service providers;

(b) Mapping of the role, nature and functions of the private sector, including service providers;

(c) Practices in the prevention and investigation of cybercrime by the private sector;

(d) Practices relating to cooperation between the private sector and law enforcement in the prevention and investigation of cybercrime;

(e) Ability of national and multinational service providers to assist law enforcement in the prevention and investigation of cybercrime;

(f) Allocation of costs of cybercrime;

(g) Evaluation of the strengths and weaknesses of existing approaches.

Topic 10. Crime prevention and criminal justice capabilities and other responses to cybercrime

Background

44. The debate about response to cybercrime often focuses on the legal response, but anti-cybercrime strategies generally follow a more comprehensive approach.

Other responses

45. In addition to legal responses to cybercrime, other responses to cybercrime include the adoption of crime prevention measures, the development of the necessary infrastructure to investigate and prosecute offences (e.g. equipment and personnel), the training of experts involved in the fight against cybercrime, the development of best practices, the education of Internet users and the technical solutions to prevent or investigate cybercrime.

Scope of the study

46. The study on this topic will consist of the following:

(a) Overview of other approaches used to respond to cybercrime;

(b) Measures to prevent cybercrime;

(c) Determination of the means to measure the success of these approaches;

(d) Analysis of the relationship between the different responses and the possibilities for adopting them in combination;

(e) Possible role of academia, particularly through development of appropriate curricula and research on the phenomenon of cybercrime.

Topic 11. International organizations

Background

47. In the 1970s and 1980s, legal approaches to cybercrime were largely made at the national level. In the 1990s, the issue of cybercrime began to be addressed within regional and international organizations, including through the General Assembly, which, over the years has adopted several resolutions on cybercrime,[56] the Commonwealth (Model Law on cybercrime and the potential expansion of the Harare Scheme to cover electronic data), the Council of Europe (Convention on Cybercrime), the European Union (Framework Decision on attacks against

[56] For example, General Assembly resolutions 45/121, 55/63, 56/121 and 60/177.

information systems and the Convention established by the Council in accordance with article 34 of the Treaty on European Union, on mutual assistance in criminal matters between the member States of the European Union), the Commonwealth of Independent States (CIS) (2001 agreement on cooperation of CIS countries to combat crimes in the sphere of computer information), the Organization of American States and the Shanghai Cooperation Organization. International organizations, including the International Telecommunication Union, which has undertaken activities within the framework of the Global Cybersecurity Agenda, and the United Nations Office on Drugs and Crime have collected data and prepared studies.

Harmonization of standards

48. Single unified standards with regard to technical protocols have proved to be successful and raise the question of how conflicts between different international approaches can be avoided.[57] The Council of Europe Convention on Cybercrime and the Commonwealth Model Law on cybercrime have both adopted the most comprehensive approach, as they cover substantive criminal law, procedural law and international cooperation. An examination of existing frameworks to identify their scope, strengths, weaknesses and any possible gaps could be undertaken under this topic.

Scope of the study

49. The study on this topic will consist of:

(a) Inventory of best practices from regional and international organizations, including the United Nations;

(b) Strengths and weaknesses of existing approaches;

(c) Gap analysis of existing international legal approaches.

Topic 12. Technical assistance

Background

50. Contrary to what is sometimes believed, cybercrime is not a problem that mainly affects developed countries. In 2005, the number of Internet users in developing countries surpassed the number in industrial nations for the first time.[58] Since one of the fundamental aims of anti-cybercrime strategies is to prevent users from becoming victims of cybercrime, the importance of fighting cybercrime in developing countries cannot be underestimated. It is also critical to take into account the fact that the impact of cybercrime on developing and developed countries may be different. In 2005, the Organization for Economic Cooperation and Development published a report analysing the impact of spam on developing countries[59] and found that developing countries often report that their Internet users

[57] For details see M. Gercke, “National, regional and international legislative approaches in the fight against cybercrime”, *Computer Law Review International*, 2008, pp. 7 ff.

[58] See Development Gateway’s Special Report, *Information Society — The Next Steps* (2005).

[59] “Spam issues in developing countries” (see footnote 34 above).

suffer more than users in developed countries from the impact of spam and Internet abuse.

Technical assistance

51. The transnational dimension of cybercrime requires all countries to act in an effective and coordinated manner. Developed and developing countries share an equal interest in the provision of technical assistance. Preventing the establishment of safe havens for cybercrime offenders is one of the key challenges in the fight against cybercrime.[60] Capacity-building in developing countries to allow them to combat cybercrime has therefore become a major task for the international community.

52. The importance of technical assistance is reflected in the Salvador Declaration, adopted by the Twelfth United Nations Congress on Criminal Prevention and Criminal Justice in 2010, in which it recommended that the United Nations Office on Drugs and Crime should provide, on request, technical assistance to States in addressing cybercrime. It also proposed that an action plan for capacity-building at the international level be given consideration, to be developed with all relevant partners. Technical assistance should be kept up to date and provided on an ongoing basis.

Scope of the study

53. The study on this topic will consist of:

(a) Identification of fundamental elements and principles of technical assistance in addressing cybercrime;

(b) Inventory of existing cybercrime training courses at the national, regional and international levels;

(c) Identification of best practices in providing technical assistance relating to cybercrime.

[60] This issue was addressed by a number of international organizations. General Assembly resolution 55/63 points out: “States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies”. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The principles and action plan to combat high-tech crime endorsed at the Meeting of Justice and Interior Ministers of the Group of Eight, held at Washington, D.C., on 10 December 1997 highlights: “There must be no safe havens for those who abuse information technologies”.

Annex II

Methodology for the study

1. In order to achieve the mandate of the expert group regarding the study, the structure set out below has been elaborated to facilitate the conduct of the study, which will be carried out under the auspices of the expert group.

2. Each country will have the right to present its views, which should be reflected in the study.

3. The United Nations Office on Drugs and Crime (UNODC) will be tasked with developing the study, including developing a questionnaire, collecting and analysing data and developing a draft text of the study. To accomplish this task, UNODC will draw upon its internal expertise and capacity from across the various thematic branches of UNODC (Division for Treaty Affairs, Policy and Research Branch). For that purpose, adequate extrabudgetary resources should be made available to enable UNODC to discharge these functions efficiently. In order to help the Secretariat ensure that major technological expertise, systems and needs are adequately represented, each regional group will provide to the Secretariat names of governmental experts (not more than six), their contact information and their areas of expertise. The Secretariat will consult with the experts as a resource on an ad hoc basis, as appropriate.

4. The Secretariat will regularly brief and consult the Bureau of the expert group on the process and circulate to Member States the minutes of the consultations. The development of the list of experts is not intended to create any closed-ended expert group or other parallel or subsidiary bodies of the expert group.

5. For the information-gathering, UNODC will prepare a questionnaire for further dissemination to Member States, intergovernmental organizations and private sector entities (see the indicative timeline below), which will consist of a single survey instrument based on the outlines contained in the concept/working paper of the first meeting of the expert group, as amended, and on the recommendations of the first meeting of the expert group, as reflected in its report.

6. Secondarily, and as needed, the Secretariat, bearing in mind the need to have balanced representation of different regions, will consult with representatives from the private sector, including representatives of Internet service providers, users of services and other relevant actors; representatives from academia, from both developed and developing countries; and representatives from relevant intergovernmental organizations.

Indicative timeline

January 2011: Policy directions and guidelines provided by the first meeting of the expert group. Endorsement of the topics, methodology and timeline of the study.

February-April 2011: Identification of the experts assisting UNODC in the conduct of the study (see above). Submission of names to the Bureau of the expert group. Communication of names of governmental experts through the regional groups.

April 2011: Twentieth session of the Commission on Crime Prevention and Criminal Justice. Distribution of a draft UNODC questionnaire for information-gathering. Request for feedback/comments from Member States. Online consultations to receive comments from expert group members. Commission's recognition of the results of the first meeting of the expert group and the future work, as proposed at the first meeting.

Mid-June 2011: Deadline for receiving comments on the questionnaire.

Mid-July 2011: Finalization of the questionnaire and dissemination to Member States. The questionnaire will also be sent, through separate letters, to intergovernmental organizations and representatives from the private sector and academic institutions, who will be invited to provide information and respond to questions that are of relevance for them. Especially for the private sector, assurances will be provided that any data received will remain confidential and, if published, anonymous.

Mid-July-late December 2011: Data collection and classification (5.5 months, with a midterm reminder to be sent by the Secretariat in early October 2011).

Early December 2011: Second meeting of the expert group, in conjunction with the reconvened twentieth session of the Crime Commission. Briefing on progress made. Interim progress report for the information of the Crime Commission at its twenty-first session (April 2012).

April 2012: Submission of interim progress report to the Crime Commission at its twenty-first session.

Mid-January 2012-July 2012: Analysis of data and drafting of the study. Finalization of draft text of the study.

August 2012: Dissemination of draft text of the study to expert group members to ensure timely preparation for the third meeting of the expert group.

October 2012: Third meeting of the expert group, to review, revise and adopt the draft study.

April 2013: Submission of the study to the Crime Commission at its twenty-second session for its consideration.