20 December 2010

Original: English

Expert group on cybercrime
Vienna, 17-21 January 2011

Draft topics for consideration in a comprehensive study on the 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.

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 responses).

V.10-58677 (E)

4. In order to draft a structure for the study, these three dimensions (substantive aspects, perspective and focus) have been converted into 13 topics that follow the mandate of the Declaration. The 13 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) Cybercrime offences (topic 1);

(b) Statistics (topic 2);

(c) Challenge 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, five specific areas of legal responses are identified:

(a) Harmonization of legislation (topic 4);

(b) Substantive criminal law (topic 5);

(c) Investigative instruments (topic 6);

(d) International cooperation (topic 7);

(e) Electronic evidence (topic 8);

(f) Liability (topic 9).

Non-legal 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.

Response by the international community (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.

Response by the private sector (topic 13)

10. As already noted, the Salvador Declaration also recommends that the comprehensive study contain an analysis of the response by the private sector.

II. Detailed overview of topics

Topic 1. Phenomenon of cybercrime

Background

11. Computer crime and, more specifically, cybercrime are terms used to describe a specific category of criminal conduct. The offences range from illegal content to certain forms of economic crime. 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

12. 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

---

[1] Regarding the related challenges, see Slivka/Darrow; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, p. 217 et seq.

[2] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, p. 217 et seq.

[3] Gemignani, Computer Crime: The Law in ‘80, Indiana Law Review, vol. 13, 1980, p. 681.

[4] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, p. 217 et seq.

[5] Freed, Materials and cases on computer and law, 1971, p. 65.

[6] Bequai, The Electronic Criminals — How and why computer crime pays, Barrister, vol. 4, 1977, p. 8 et seq.

[7] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, p. 225 et seq; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

[8] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, p. 217 et seq; Bequai, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, vol. 6, 1977, p. 22.

[9] Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, p. 73.

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 methods of criminal conduct. The distribution of child pornography, 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

13. 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 not yet criminalized;

(c) Overview of combined offences (such as "phishing") and future trends;

---

[10] BloomBecker, The Trial of Computer Crime, Jurimetrics Journal, vol. 21, 1981, p. 428; Schmidt, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, vol. 21, 1981, p. 345 et seq. Denning, Some Aspects of Theft of Computer Software, Auckland University Law Review, vol. 4, 1980, p. 273 et seq; Weiss, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review,
vol. 11, 1983, p. 1 et seq; Bigelow, The Challenge of Computer Law, Western England Law Review, vol. 7, 1985, p. 401; Thackeray, Computer-Related Crimes, Jurimetrics Journal, 1984, p. 300 et seq.

[11] Yee, Juvenile Computer Crime — Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, vol. 7, 1984, p. 336 et seq; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, vol. 8, 1985, p. 89 et seq; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review, vol. 33, 1984, p. 777 et seq.

[12] Child Pornography, CSEC World Congress Yokohama Conference, 2001, p. 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, United States House of Representatives, 109th Congress, 2007, p. 9.

[13] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term 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 Understanding Cybercrime: A Guide for Developing Countries, International Telecommunication Union 2009, chapter 2.8.4.

[14] "Botnets" is a short term for a group of compromised computers running software under external control. For more details, see Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, p. 4.

[15] Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006.

[16] Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, p. 499 et seq.

(d) Inventory of relevant cases;

(e) Definition and typology of cybercrime;

(f) Crime prevention mechanisms (technical);

(g) Examination of the importance of the definition of cybercrime;

(h) Considerations regarding the possibility of decriminalization as a solution to certain cybercrime offences.

Topic 2. Statistical information

Background

14. 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

15. 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 data from 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]

16. Secondly, statistics can reflect only crimes that have been detected and reported.[22] Especially with regard to cybercrime, there are concerns that the number

---

[17] Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, p. 308, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[18] Regarding the emerging importance of crime statistics, see Osborne/Wernicke, Introduction to Crime Analysis, 2003, p. 1 et seq, available at www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

[19] See, in this context, Overcoming barriers to trust in crimes statistics, United Kingdom Statistics Authority, 2009, p. 9, available at www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

[20] Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, p. 168, available at 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, Oct. 2006, p. 3.

[22] Regarding the related challenges see Kabay, Understanding Studies and Surveys of Computer Crime, 2009, available at www.mekabay.com/methodology/crime_stats_methods.pdf.

of unreported cases appears to be significant.[23] Businesses may fear that negative 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

17. 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;

---

[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 Heise News, 27.10.2007, available at www.heise-security.co.uk/news/80152. See also Comments on Computer Crime — Senate Bill S. 240, Memphis State University Law Review, 1980, p. 660.

[24] See Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, available at www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, p. 310, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[25] See Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, p. 310, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, p. 2, available at www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

[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, 09.10.2007, available at www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin, as well as the information provided on the INTERPOL website, available at www.interpol.int/Public/THB/vico/Default.asp.

[27] See SOCA, "International crackdown on mass marketing fraud revealed, 2007", available at www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[28] In the 2006 NW3C Internet Crime report, 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 in those offences is high.

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

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

(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

18. 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

19. 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; Information Security — Computer Controls over Key Treasury Internet Payment System, GAO 2003, p. 3; Sieber, Council of Europe Organised Crime Report 2004, p. 143.

[30] Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", p. 9.

[31] For a brief history of the Internet, including its military origins, see Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff, "A Brief History of the Internet", available at www.isoc.org/internet/history/brief.shtml.

[32] Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

Scope of the study

20. 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. Harmonization of legislation

Background

21. 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

22. 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]

23. As cybercrime is a truly transnational crime,[37] international cooperation is an essential requirement for successful investigations and prosecutions.[38] Effective

---

[33] Understanding Cybercrime: A Guide for Developing Countries, International Telecommunication Union 2009, chapter 2.6.7.

[34] See Spam Issue in Developing Countries, p. 4, available at www.oecd.org/dataoecd/5/47/34935342.pdf.

[35] Regarding the principle of freedom of speech, see Tedford/HerbeckHaiman, Freedom of Speech in the United States, 2005; Barendt, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; Emord, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance, see Woo/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, p. 530 et seq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; Volokh, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, vol. 33, 2001, p. 57 et seq, available at www.law.ucla.edu/volokh/harass/religion.pdf; Cohen, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at www.fas.org/sgp/crs/misc/95-815.pdf.

[36] Concerns over freedom of expression explain why certain acts of racism were not made illegal by the Convention on Cybercrime, but their criminalization was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

[37] Regarding the extent of transnational attacks in the most damaging cyber attacks, see Sofaer/Goodman, Cyber Crime and Security — The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 7, available at http://media.hoover.org/documents/0817999825_1.pdf.

international cooperation requires a degree of common understanding and the harmonization of legislation in order to prevent the establishment of safe havens.[39]

Scope of the study

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

(a) Analysis of the success and limitations of existing efforts to harmonize cybercrime legislation;

(b) 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;

(c) Analysis of the extent to which differences in legal standards affect international cooperation;

(d) Identification of techniques in legislative drafting that ensure the necessary flexibility to maintain fundamental legal traditions within the process of harmonization.

Topic 5. Criminalization of cybercrime offences

Background

25. 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.

Substantive criminal law

26. 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 approaches go further, however, and criminalize offences such as the production and distribution of tools (such as software or hardware) that can be used to commit cybercrime, acts related to child pornography, “grooming” or hate speech.

---

[38] Regarding the need for international cooperation in the fight against cybercrime see Putnam/Elliott, International Responses to Cyber Crime, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 35 et seq, available at http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security — The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 1 et seq, available at http://media.hoover.org/documents/0817999825_1.pdf.

[39] Regarding the dual criminality principle in international investigations, see United Nations Manual on the Prevention and Control of Computer-Related Crime, p. 269, available at www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, p. 5, available at www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

Scope of the study

27. The study on this topic will build upon the findings of the study on topic 1, on the phenomenon of cybercrime, and will consist of the following:

(a) Inventory of national and regional approaches to the criminalization of cybercrime;

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

(c) Analysis of differences in the approach of common-law and civil-law countries to the criminalization of cybercrime.

Topic 6. Investigation procedures

Background

28. 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]

Investigative measures

29. 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.

30. Some States have adopted measures beyond these standard provisions to address specific challenges such as the interception of VoIP communication.[42]

---

[40] Regarding user-based approaches in the fight against cybercrime, see Görling, The Myth Of User Education, 2006, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See as well the comment made by Jean-Pieree Chevenement, French Minister of the Interior, at the G-8 Conference 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] Owing to the protocols used in Internet communication and to worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Owing 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, International Telecommunication Union 2009, chapter 3.2.7.

[42] The term "voice over Internet protocol" is use to describe the transmission technology for delivering voice communication by using packet-switched networks and related protocols. For more information see Swale, Voice Over IP: Systems and Solutions, 2001; Black, "Voice Over IP", 2001.

Although most States have provided for investigation measures, such as wiretapping, that enable them to intercept landline as well as mobile phone communications,[43] these measures are usually not sufficient to allow for the interception of VoIP communications. The interception of traditional voice calls is usually carried out through telecommunications providers.[44] Applying the same principle to VoIP, law enforcement agencies generally operate through Internet service providers and service providers supplying VoIP services. If, however, the VoIP service is based on peer-to-peer technology, service providers may be unable to intercept communications.[45]

Scope of the study

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

(a) 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 with regard to specific investigative provisions relating to cybercrime;

(d) Analysis of differences in the approach to investigative provisions relating to cybercrime in common-law and civil-law countries.

Topic 7. International cooperation

Background

32. An increasing number of cybercrimes have an international dimension,[46] particularly owing to the fact that offenders, operating through the transnational

---

[43] Regarding the importance of interception and the technical solutions, see Karpagavinayagam/State/Festor, "Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection", ICIMP 2007. Regarding the challenges related to interception of data communication, see SwaleChochliouros/Spiliopoulou/Chochliouros, "Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism — The European Response", in Janczewski/Colarik, "Cyber Warfare and Cyber Terrorism", 2007, p. 424.

[44] Regarding the differences between PSTN and VoIP communication, see Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, p. 217 et seq.

[45] Regarding the interception of VoIP by law enforcement agencies, see Bellovin and others, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP"; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006; Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, p. 217 et seq.

[46] Regarding the transnational dimension of cybercrime, see Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law and Policy, vol. 12, No. 2, p. 289, available at www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. Sofaer/Goodman, Cyber Crime and Security — The Transnational Dimension in Sofaer/Goodman, The

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.[47] 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 on international cooperation available to States.[48]

Instruments for international cooperation

33. There are four main sources of the legal basis necessary for formal international cooperation in forms such as extradition, mutual legal assistance in criminal matters and cooperation for the purposes of confiscation.

34. First, provisions on international cooperation may form a part of international and regional agreements that address a particular international crime, such as the United Nations Convention against Transnational Organized Crime[49, 50] and the Council of Europe Convention on Cybercrime.[51] Second, there are regional treaties on international cooperation, such as the Council of Europe, Inter-American and Southern African Development Community conventions on extradition or mutual legal assistance in criminal matters. The third source is bilateral agreements on extradition or mutual legal assistance. Those agreements, in general, contain specific information relating to the types of requests that can be submitted, define the relevant procedures and modes of contact, as well as rights and obligations of the requesting and requested States.[52] The fourth source for international cooperation is domestic law, which may allow international cooperation on a reciprocal or a case-by-case basis.

Scope of the study

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

Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 1 et seq, available at http://media.hoover.org/documents/0817999825_1.pdf.

47 See in this context Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, p. 217, available at www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

48 Gabuardi, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, vol. I, No. 2, p. 156, available at http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

49 Regarding the Convention, see Smith, An International Hit Job: Prosecuting Organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, vol. 97, p. 1118, available at www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

50 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at www.oas.org/juridico/english/sigs/a-55.html.

51 Council of Europe Convention on Cybercrime, ETS 185.

52 See in this context the United Nations Model Treaty on Mutual Assistance in Criminal Matters, 1990, resolution 45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, p. 217, available at www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

(a) Challenges with regard to international cooperation in cybercrime cases;

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

(c) Inventory of best-practice examples from bilateral agreements;

(d) Inventory of cybercrime cases involving international cooperation;

(e) Role of informal means of cooperation, such as intelligence-sharing;

(f) Overview of the current needs of the relevant authorities with regard to international cooperation.

Topic 8. Electronic evidence

Background

36. 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[53] and the low cost[54] of the storage of digital documents as compared to the storage of physical documents have led to a growth in the number of digital documents.[55] Today, a significant amount of data is stored only in digital form.[56] As a consequence of this increase, electronic documents such as text documents, digital videos and digital pictures[57] are playing a role in cybercrime investigations and related court proceedings.[58]

---

[53] See Abramovitch, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, vol. 22, Issue 3, p. 28 et seq; Coughlin/Waid/Porter, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[54] Giordano, Electronic Evidence and the Law, Information Systems Frontiers, vol. 6, No. 2, 2006, p. 161; Willinger/Wilson, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, 2004, vol. X, No. 5.

[55] Lange/Minster, Electronic Evidence and Discovery, 2004, p. 6.

[56] Homer, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, vol. 1, No. 1, p. 1, available at www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[57] Regarding the admissibility and reliability of digital images, see Kwiatkowski, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law and Policy, p. 267 et seq.

[58] Harrington, A Methodology for Digital Forensics, T. M. Cooley J. Pac. and Clinical L., 2004, vol. 7, p. 71 et seq; Casey, Digital Evidence and Computer Crime, 2004, p. 14. Regarding the legal frameworks in different countries, see Rohrmann/Neto, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Wang, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Bazin, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; Makulilo, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5. Winick, Search and Seizures of Computers and Computer Data, Harvard Journal of Law and Technology, 1994, vol. 8, No. 1, p. 76; Insa,

Rules for electronic evidence

37. Electronic evidence presents a number of challenges, at both the stage of its collection and that of its admission as evidence.[59] 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 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.[60]

38. Digitalization also influences the way in which law enforcement agencies and courts deal with evidence.[61] 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.[62]

Scope of the study

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

(a) Inventory of provisions dealing with the handling and admissibility of electronic evidence;

(b) Analysis of differences in the approach and the identification of common principles in relation to electronic evidence in common-law and civil-law countries.

Topic 9. Liability of Internet service providers

Background

40. 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.[63] The situation is similar with regard to

---

Situation Report on the Admissibility of Electronic Evidence in Europe, in Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, p. 213.

[59] Casey, Digital Evidence and Computer Crime, 2004, p. 9.

[60] Regarding the need for a formalization of computer forensics, see Leigland/Krings, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, vol. 3, No. 2.

[61] Regarding the difficulties of dealing with digital evidence on the basis of the traditional procedures and doctrines see 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, p. 57 et seq.

[62] See Vacca, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 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, p. 291 et seq.

[63] Regarding the network architecture and the consequences with regard to the involvement of service providers, see Black, Internet Architecture: An Introduction to IP Protocols, 2000;

the downloading of films that contain child pornography. 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.

Role of the Internet service provider

41. 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 Internet providers should be limited.[64] The answer to the question is critical for the economic development of the information and communications technology infrastructure.

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

Scope of the study

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

(a) Inventory of approaches to regulate the responsibility of Internet service providers by differentiating between the different types of Internet service providers;

(b) Concept of the limitation of responsibility of Internet service providers;

(c) Ability of Internet service providers to assist law enforcement and prevent cybercrime.

Topic 10. Non-legal responses to cybercrime

Background

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

Non-legal responses

45. Non-legal responses to cybercrime include, for example, 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

---

Zuckerman/McLaughlin, Introduction to Internet Architecture and Institutions, 2003, available at http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[64] For an introduction into the discussion see Elkin-Koren, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, vol. 9, 2005, p. 15 et seq, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

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 non-legal approaches used to respond to cybercrime;

(b) Determination of the means to measure the success of those approaches;

(c) Analysis of the relationships between the different non-legal responses and the possibilities for adopting them in combination.

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,[65] the Commonwealth (Model Law on Cybercrime), the Council of Europe (Convention on Cybercrime) and the European Union (Framework Decision on Attacks against Information Systems).

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.[66] 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;

(b) Strengths and weaknesses of existing approaches;

(c) Gap analysis of existing international legal approaches.

Topic 12. Technical assistance

---

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

[66] For details see Gercke, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, p. 7 et seq.

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.[67] 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 Organisation for Economic Cooperation and Development published a report analysing the impact of spam on developing countries[68] and found that developing countries often report that their Internet users 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 coordination. Preventing the establishment of safe havens for cybercrime offenders is one of the key challenges in the fight against cybercrime.[69] Capacity-building in developing countries to allow them to combat cybercrime has therefore become a major task for the international community. This is reflected in the Salvador Declaration, adopted by the Twelfth United Nations Congress on Crime 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.

Scope of the study

52. The study on this topic will consist of:

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

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

Topic 13. Private sector

Background

---

[67] See “Development Gateway’s Special Report, Information Society — Next Steps?”, 2005, available at http://topics.developmentgateway.org/special/informationsociety.

[68] “Spam Issue in Developing Countries”, available at www.oecd.org/dataoecd/5/47/34935342.pdf.

[69] This issue was addressed by a number of international organizations. The General Assembly stated in its resolution 55/63: “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 G-8 10-point action plan highlights: “There must be no safe havens for those who abuse information technologies”.

53. The prevention and investigation of cybercrime depends on a number of different elements. While emphasis is often placed on ensuring adequate legislation, the 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.

Role of industry

54. 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

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

(a) Inventory of best practices in the prevention and investigation of cybercrime by the private sector;

(b) Analysis of the requirements of industry and of law enforcement;

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