21 January 2010

Original: English

Expert group on cybercrime
Vienna, 17-21 January 2011

Working Paper
Draft collection of topics for consideration within a comprehensive study on impact 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. This 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, the comprehensive study is to examine the following topics:

> 42. *We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct 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.*

3. Paragraph 42 of the Salvador Declaration thus identifies the various substantive aspects which the study should investigate (e.g. the problem of cybercrime, national legislation, best practices, technical assistance and international cooperation) but also the perspective (e.g. the response by Member States, the international community and the private sector) and the focus (e.g. 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 thirteen topics that follow the mandate of the Declaration. These thirteen topics are grouped below into subcategories.

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 into 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 to other types of responses to cybercrime. Those activities are covered in this section (topic 10).

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 within the sections dealing with legal responses, a separate section addressing the responses of the international community will facilitate the analysis of more general aspects such as the relation between regional and international approaches (topic 11).

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 (topic 12).

II. Detailed overview of topics

Topic 1. Phenomenon of cybercrime

Background

10. Computer crime or, cybercrime are terms used to describe specific categories 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 the physical damage of 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] which 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]

---

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

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

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

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

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

[6] Bequai, The Electronic Criminals – How and why computer crime pays, Barrister, Vol. 4, 1977, page 8 et seq.

[7] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, page 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, page 217 et seq; Bequai, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, page 22.

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 (www= World Wide Web) in the 1990s that was followed by a rapidly growing number of Internet users led to new 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 attacks"[14] and emerging uses of technology such as "Voice-over-IP (VoIP) communication"[15] and "Cloud Computing",[16] which create difficulties for law enforcement.

Scope of the study

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

---

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

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

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

[12] Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, U.S. House of Representatives, 109th Congress, 2007, page 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" linked to popular hacker naming conventions. For more information see: Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, Chapter 2.8.4.

[14] Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 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, page 499 et seq.

(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.

Topic 2. Statistical information

Background

13. Crime statistics provide the basis for discussion and decision-making processes by policymakers and academics.[17] Further, 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] Both sources present challenges when they are used to develop policy recommendations. First of all, crime statistics are generally created on 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 as a separate figure.[21]

15. Secondly, statistics can only contain 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, page 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 crimes statistics see: Osborne/Wernicke, Introduction to Crime Analysis, 2003, page1 et seq, available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

[19] See in this context: Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009, page 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, page 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, page 3.

[22] Regarding the related challenges see Kabay, Understanding Studies and Surveys of Computer

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, these 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 only lost small amounts, victims may prefer not to go through with time-consuming reporting procedures to law enforcement. In practice, those cases that are reported often involve extremely high fees.[28]

Scope of the study

16. (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;

Crime, 2009, available at: www.mekabay.com/methodology/crime_stats_methods.pdf.

[23] "The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT 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's 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, page 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, page 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, page, 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, page 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", The 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 USD losses were related to the Nigerian Letter Fraud, but those cases that were reported had an average loss of 5,100 USD each. The number of reported offences is very low, while the average loss of those offences is high.

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

(e) Evaluation of 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

17. A lot of attention is currently being paid to the development of strategies to address the specific challenges of cybercrime. The reasons for this development are twofold: firstly, that some of the instruments required to investigate cybercrime are new and therefore require intensive research, and secondly, that investigating crimes involving network technology is accompanied by several unique challenges as compared with 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 software 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 in 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 through 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 preserve 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", page 11; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3; Sieber, Council of Europe Organised Crime Report 2004, page 143.

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

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

(b) Summary of best practices, both technical and legal, on how to address these 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 lies in the fact 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 more scarce and expensive resources.[34] In terms of illegal content, some countries and regions may criminalize the dissemination of material that may be considered as protected by the principle of freedom of speech[35] in others.[36]

22. 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, ITU 2009, Chapter 2.6.7.

[34] See Spam Issue in Developing Countries, Page 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 & Technology, Vol. 15, No. 2, 2002, page 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, page 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 (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, 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, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[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

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. (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 of which techniques can help to ensure consistency in the approaches;

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

Topic 5. Criminalization

Background

24. The effective investigation and prosecution of cybercrime will require the creation 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

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, 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.

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

Dimension of Cyber Crime and Terrorism, 2001, page 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, page 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, 269, available at: www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

(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 to 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

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

---

[40] Regarding the elements of a anti-cybercrime strategy see above: xxx. 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 Interior, at the G8 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] 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, ITU 2009, Chapter 3.2.7.

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

(c) Overview of the current demands 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 due 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 in the location between 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 amongst States can make international cooperation difficult, as can the relatively limited number of treaties and agreements on international cooperation available to States.[44] Furthermore, it should be discussed and agreed upon what should be considered as an international matter in cybercrime cases.

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.

Such provisions on international cooperation may form a part of international and regional agreements including the United Nations Convention against Transnational Organized Crime (Organized Crime Convention).45

---

[42] Regarding the transnational dimension of cybercrime see: Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, No. 2, page 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 Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq, available at: http://media.hoover.org/documents/0817999825_1.pdf.

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

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

[45] Convention against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003; Regarding the Convention see: Smith, An International Hit Job: Prosecuting

Scope of the study

33. (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, inter alia, 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 demands 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.

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

---

Organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

[46] With regard to the development see: Abramovitch, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 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.

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

number of digital documents.[48] Today, a significant amount of data is only stored 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 evidence sources such as fingerprints or witness identification is 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 and other discovered data.[55]

---

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

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

[50] 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 & Policy, page 267 et seq.

[51] Harrington, A Methodology for Digital Forensics, T.M. Cooley J. Pac. & Clinical L., 2004, Vol. 7, page 71 et seq; Casey, Digital Evidence and Computer Crime, 2004, page 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 & Technology, 1994, Vol. 8, No. 1, page 76; Insa, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213.

[52] Casey, Digital Evidence and Computer Crime, 2004, page 9.

[53] 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.

[54] 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, page 57 et seq.

[55] See Vacca, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 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, page 291 et seq.

Scope of the study

37. (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 digital evidence exchange cross-border.

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.63 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.

39. 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.

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 addressed. 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 very often focuses on legal responses, but anti-cybercrime strategies generally follow a more comprehensive approach and include a number of other responses.

Other responses

45. In addition to legal responses to cybercrime, other response 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. (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 of adopting them in combination

(e) Possible role of academia particularly through development of appropriate curriculum 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 United Nations 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 (the EU Framework Decision on Attacks against 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 (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 Telecommunications Union (ITU), which has undertaken activities within the framework of the Global Cybersecurity Agenda (GCA), and UNODC have collected data and prepared studies.

Harmonization of standards

48. Single unified standards with regard to technical protocols have proven 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

---

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

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

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. (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 becoming victims of cybercrime, the importance of fighting cybercrime in developing countries cannot be underestimated. It is also critical that the fact that the impact of cybercrime on developing and developed countries may be different is taken into account. In 2005, the OECD published a report analyzing the impact of spam on developing countries[59] and found that developing countries often report that their Internet users suffer more 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 resolution of the Twelfth United Nations Congress on Criminal Prevention and Criminal Justice in 2010 which recommended that the United Nations Office on Drugs and Crime

---

[58] See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[59] "Spam Issue in Developing Countries", available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[60] This issue was addressed by a number of international organisations. The UN 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 G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies".

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. This would 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. (a) Identification of fundamental elements and principles of technical assistance and capacity-building in addressing cybercrime;

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

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