United Nations A/CONF.213/9

Twelfth United Nations Congress on Crime Prevention and Criminal Justice

Salvador, Brazil, 12-19 April 2010

Distr.: General
22 January 2010

Original: English

Item 8 of the provisional agenda*
Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime

Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime

Working paper prepared by the Secretariat

I. Introduction

1. The fact that cybercrime figures prominently on the agenda of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice highlights its undiminished importance and the serious challenges it poses, despite the fact that a debate on the issue has been going on for almost half a century.

2. Over the past 50 years, various solutions have been discussed and developed to address the issue of cybercrime. In part, the topic remains challenging because the technology is constantly developing and because the methods used to commit cybercrime are also changing.

3. From the 1960s to the 1980s, States were confronted with new acts such as computer manipulation and data espionage that were often not covered by existing criminal legislation. The discussion at that time focused on the development of a legal response.[1]

4. The introduction of a graphical interface in the 1990s, which was followed by a rapidly growing number of Internet users, led to new challenges. Information legally posted in one country was available globally, even in countries where the publication of such information was not legal. Another concern relating to online

---

* A/CONF.213/1.

[1] See: Susan H. Nycum, *The Criminal Law Aspects of Computer Abuse: Applicability of the State Penal Laws to Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1976) and Ulrich Sieber, *Computerkriminalität und Strafrecht* (Cologne, Karl Heymanns Verlag, 1977).

V.10-50382 (E) 100210 110210

services was the speed of information exchange, which proved to be especially challenging in the investigation of crime with transnational dimensions.[2]

5. The first decade of the twenty-first century has been dominated by new and sophisticated methods of committing crimes (such as "phishing",[3] and "botnet attacks"[4]) and by the use of technologies that are even more difficult for law enforcement officers to handle within investigations (such as Voice-over-Internet-Protocol communication and "cloud computing").

II. The challenges of cybercrime

A. Uncertainty of extent

6. Despite technological improvements and intensive investigations, the degree to which information technology is used for illegal purposes remains stable or may even be growing. Some e-mail providers have reported that as many as 75 to 90 per cent of all e-mails are spam.[5] Similar figures of constant or growing numbers are published for other, more widespread criminal conduct as well. For example, the Internet Watch Foundation, in its 2008 Annual and Charity Report, shows a rather stable number of confirmed commercial child pornography websites between 2006 and 2008.

7. While statistical information is useful for drawing attention to the existing or growing importance of the issue, one of the major challenges related to cybercrime is the absence of reliable information about the extent of the problem as well as about arrests, prosecutions and convictions. Crime statistics often do not list offences separately while the few statistics on the impact of cybercrime that are available are, in general, insufficiently detailed to provide policymakers with reliable information about the scale or extent of offences.[6] Without such data, it is

---

[2] Regarding the impact on cybercrime investigations of the heightened speed with which data were exchanged, see: International Telecommunications Union, *Understanding Cybercrime: A Guide for Developing Countries* (Geneva, 2009). Available from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

[3] As described by the International Telecommunication Union in *Understanding Cybercrime: A Guide* (see footnote 2), "phishing" is an act that is carried out to make the victim disclose personal or secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions.

[4] A "botnet" is a group of compromised computers running a software under external control. See Clay Wilson, "Botnets, cybercrime and cyberterrorism: vulnerabilities and policy issues for Congress", Congressional Research Service Report RL32114, updated on 29 January 2008, available from www.fas.org/sgp/crs/terror/RL32114.pdf.

[5] The Messaging Anti-Abuse Working Group reported in 2009 that between 85 and 90 per cent of all e-mails were spam (http://www.maawg.org/sites/maawg/files/news/2009_MAAWG-Consumer_Survey-Part1.pdf).

[6] United States of America, Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO report GAO-07-705 (Washington, D.C., June 2007), p. 22; and Ian Walden, *Computer Crimes and Digital Investigations* (Oxford, Oxford University Press, 2007).

difficult to quantify the impact of cybercrime on society and develop strategies to address the issue.[7]

8. One of the reasons why statistical information is missing is that it is difficult to estimate the extent of the financial loss and the number of offences committed by cybercriminals. Some sources estimate losses to businesses and institutions in the United States[8] due to cybercrime to be worth as much as 67 billion United States dollars a year; however, it is uncertain if the extrapolation based on sample survey results is justifiable.[9] This methodological criticism applies not only to the losses, but also to the number of recognized offences.[10] The extent to which victims report cybercrime is also uncertain. Although authorities engaged in the fight against cybercrime encourage victims to report these crimes, there is a concern that in the financial sector in particular victims (e.g. banks) do not report occurrences of such crime for fear that negative publicity could damage their reputation.[11] If a company announces that hackers have accessed their server, customers may lose faith and the full costs and consequences could be even greater than the losses caused by the hacking attack. In addition, targets may not believe that law enforcement agencies will be able to identify offenders. However, if offenders are not reported and prosecuted, offenders may go on to reoffend.

9. Another difficulty related to statistical information is the fact that very often non-reliable or non-verifiable information is quoted repeatedly. One example of this is related to statistical information about the commercial aspects of child pornography on the Internet. In several analyses it has been quoted that child pornography on the Internet generates $2.5 billion annually worldwide.[12] Yet, the source of that figure (www.toptenreviews.com) does not provide any background information on how the research was undertaken. Given that the company says, on its website, that it "gives you the information you need to make a smart purchase. We make a recommendation for the best product in each category. Through our side-by-side comparison charts, news, articles, and videos we simplify the buying process for consumers", there are serious concerns about the reliability of the data. In another example, in 2006 a journalist for *The Wall Street Journal*[13] investigating the claim that child pornography was a business worth $20 billion a year found out that the two main documents containing information on revenues ranging from $3 billion to $20 billion (publications by the National Center for Missing and Exploited Children, in the United States, and by the Council of Europe) referred to institutions that did not confirm the numbers.

---

[7] Walden, *Computer Crimes and Digital Investigations*.

[8] United States, Federal Bureau of Investigation, *2005 FBI Computer Crime Survey*, p. 10.

[9] *Understanding Cybercrime: A Guide* (see footnote 2).

[10] Ibid.

[11] Neil Mitchison and Robin Urry, "Crime and abuse in e-business", *IPTS Report*, vol. 57, September 2001.

[12] Kim-Kwang Choo, Russel G. Smith and Rob McCusker, "Future directions in technology-enabled crime: 2007-09", Research and Public Policy Series, No. 78 (Canberra, Australian Institute of Criminology, 2007), p. 62; ECPAT International, *Violence against Children in Cyberspace* (Bangkok, 2005), p. 54; Council of Europe, *Organised Crime Situation Report 2005: Focus on the Threat to Economic Crime* (Strasbourg, December 2005), p. 41.

[13] Carl Bialik, "Measuring the child-porn trade", *Wall Street Journal*, 18 April 2006.

B. Transnational dimension

10. Cybercrime is to a large degree transnational in nature. The Internet was originally designed as a military network that was based on a decentralized network architecture. As a consequence of its underlying architecture and the global availability of services, cybercrime often has an international dimension. E-mails with illegal content are easily sent to recipients in a number of countries, even in cases where the original sender and the final recipient are both in the same country or if either the sender or the recipient uses an e-mail service operated by a provider outside the country. Some of the popular free e-mail service providers have millions of users worldwide, further highlighting the transnational dimension of cybercrime.

11. The challenges that the transnational element poses for investigating cybercrime are similar to those involved in other transnational offences. As a result of the fundamental principle of national sovereignty, according to which investigations in foreign territories cannot be carried out without the permission of local authorities, close cooperation between the States involved is crucial in cybercrime investigations. Another major challenge relates to the short time available to carry out investigations into cybercrime. Unlike illicit drugs, which, depending on the means of transportation, can take weeks to reach their destination, e-mails can be delivered in seconds and large files can be downloaded, with access to an adequate bandwidth, in minutes.

12. Timely and effective cooperation between authorities in different countries is also crucial because in cases of cybercrime the evidence is often deleted automatically and within short time frames. Protracted formal procedures can seriously hinder investigations.

13. A large number of existing mutual legal assistance agreements are still based on formal, complex and often time-consuming procedures. The establishment of procedures for quick responses to incidents and requests for international cooperation is therefore considered vital.

14. One set of principles for developing a legal framework for international cooperation in cybercrime investigations is contained in chapter III of the Convention on Cybercrime of the Council of Europe.[14] In that chapter, the increasing importance of international cooperation is addressed (art. 23-35) and the use of expedited means of communication, including fax and e-mail, are promoted (art. 25, para. 3). In addition, the parties to the Convention are called upon to designate a point of contact available 24 hours a day, seven days a week, to respond to requests for assistance by States (art. 35). Other approaches can be found in the draft international convention to enhance protection from cybercrime and terrorism and in the draft International Telecommunication Union (ITU) toolkit for cybercrime legislation.

---

[14] Council of Europe, *European Treaty Series*, No. 185. See also the "explanatory report" to that convention.

C. Differences in national legal approaches

15. One practical effect of the Internet's network architecture is that criminals committing cybercrime need not be at the scene of the crime. Preventing safe havens for criminals has therefore become a key aspect of preventing cybercrime.[15] Offenders will use safe havens to hamper investigations. One well-known example is the "Love Bug" computer worm that was developed in the Philippines in 2000[16] and reportedly infected millions of computers worldwide.[17] Local investigations were hindered by the fact that the malicious development and spreading of damaging software was not, at that time, adequately criminalized in the Philippines.

16. The issue of convergence of legislation is highly relevant, as a large number of countries base their mutual legal assistance regime on the principle of dual criminality, according to which an offence must be considered a crime both in the State requesting assistance and in the State providing it.[18] Investigations on a global level are generally limited to those acts that are criminalized in all affected countries. Although there are a number of offences that can be prosecuted anywhere in the world, regional differences play an important role. For example, different kinds of content are criminalized in different countries,[19] which means that material that can lawfully be made available on a server in one country might be considered illegal in another.[20]

17. The computer and network technology currently in use is basically the same all over the world. Apart from language issues and power adapters, there is very little difference between the computer systems and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the Internet. Due to standardization, the protocols used in countries in Africa are the same as those used

---

[15] Both the General Assembly, in its resolution 55/63, and the Group of Eight, in the principles and action plan to combat high-tech crime endorsed at the Meeting of Justice and Interior Ministers of the Group of Eight, held at Washington, D.C., on 10 December 1997 (available from www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf), have highlighted the need to eliminate safe havens for those who criminally misuse information technologies.

[16] United States, General Accountability Office, *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*, testimony given before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, United States Senate, GAO report GAO/T-AIMD-00-181 (Washington, D.C., May 2000).

[17] "Police close in on Love Bug culprit" *BBC News*, 6 May 2000. Available from http://news.bbc.co.uk/2/hi/science/nature/738537.stm.

[18] Regarding the dual criminality principle in cybercrime investigations, see the United Nations Manual on the Prevention and Control of Computer-related Crime (*International Review of Criminal Policy*, Nos. 43 and 44: United Nations publication, Sales No. E.94.IV.5), p. 269, and the background paper by Stein Schjølberg and Amanda Hubbard entitled "Harmonizing national legal approaches on cybercrime", p. 5, which was presented at the ITU Thematic Meeting on Cybersecurity held in Geneva from 28 June to 1 July 2005.

[19] The different legal approaches to regulating content is one reason why certain aspects of illegal content are not included in the Convention on Cybercrime, but are addressed in an additional protocol. See also *Understanding Cybercrime: A Guide*, chap. 2.5 (see footnote 2).

[20] With regard to the different national approaches towards the criminalization of child pornography, see, for example, Ulrich Sieber, *Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet: eine strafrechtsvergleichende Untersuchung* (Bonn, Forum Verlag Godesberg, 1999).

in the United States. Standardization enables users around the world to access the same services through the Internet.[21]

18. Two different approaches to dealing with the transnational dimension of cybercrime and differing legal standards are discussed in the paragraphs below.

1. Compatibility of legislation

19. One approach to addressing the transnational dimension of cybercrime and improving international cooperation is to develop and standardize relevant legislation. Several regional approaches have been undertaken in recent years.

20. In 2002, the Commonwealth developed a model law on computer and computer-related crime with the aim of improving legislation against cybercrime in States members of the Commonwealth and international cooperation. Without such improvements, no fewer than 1,272 bilateral treaties between Commonwealth States would be needed to cooperate across borders on this matter.[22] The model law contains provisions on substantive criminal law, procedural law and international cooperation. Due to the regional focus of the model law, the impact on harmonization is limited to States members of the Commonwealth.

21. The European Union has also made efforts to harmonize legislation on cybercrime within its 27 member States, for example through the following: directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market; Council of the European Union framework decision 2000/413/JHA on combating fraud and counterfeiting of non-cash means of payment; Council of the European Union framework decision 2004/68/JHA on combating the sexual exploitation of children and child pornography; Council of the European Union framework decision 2005/222/JHA on attacks against information systems;[23] directive 2006/24/EC of the European Parliament and of the Council of the European Union on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending directive 2002/58/EC; and Council of the European Union framework decision 2008/919/JHA amending framework decision 2002/475/JHA on combating terrorism. Unlike most other regional approaches, implementation of the instruments adopted by the European Union is mandatory for all member States. While the instruments are effective, the main obstacle to harmonization within the European Union was, at least until the beginning of 2010, the limited powers of legislation in the field of criminal law.[24] The diversity of

---

[21] Regarding the importance of single technical as well as single legal standards see: Marco Gercke, "National, regional and international approaches in the fight against cybercrime", *Computer Law Review International*, 2008, p. 7.

[22] Richard Bourne, "2002 Commonwealth Law Ministers' Meeting: policy brief", prepared for the Commonwealth Law Ministers' Meeting, held in Kingstown, Saint Vincent and the Grenadines, from 18 to 21 November 2002 (London, Institute of Commonwealth Studies, 2002), p. 9.

[23] For more information, see: Marco Gercke, "The EU framework decision on attacks against information systems", *Computer und Recht*, 2005, pp. 468 ff.; and *Understanding Cybercrime: A Guide* (see footnote 2), p. 99.

[24] Helmut Satzger, *Internationales und Europäisches Strafrecht* (Baden-Baden, Nomos, 2005), p. 84; and P.J.G. Kapteyn and Pieter Verloren van Themaat, *Introduction to the Law of the European Communities: After the Coming into Force of the Single European Act* (Boston,

approaches resulted from the fact that the European Union's ability to harmonize national criminal law was limited to special areas.[25] The Treaty of Lisbon amending the Treaty on the European Union and the Treaty establishing the European Community has changed this situation and now gives the European Union a stronger mandate to harmonize legislation on computer-related crime in the future — but this is limited to the 27 member States.

22. The Council of Europe has developed three major instruments to harmonize cybercrime legislation. The best known is the Convention on Cybercrime, which was developed between 1997 and 2001. That Convention contains provisions on substantive criminal law, procedural law and international cooperation. As at December 2009, it had been signed by 46 States and ratified by 26. Since, during the negotiation of the Convention, no agreement on criminalizing racism and the distribution of xenophobic material could be reached, the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems was introduced in 2003.[26] By December 2009, 34 States[27] had signed the Additional Protocol and 15 of them[28] had ratified it. In 2007, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[29] was opened for signature. It contains specific provisions criminalizing the exchange of child pornography, as well as the knowing obtention of access, through information and communication technologies, to child pornography (art. 20, para. 1 (f)). As at December 2009, it had been signed by 38 States,[30] three of which[31] had ratified it.

23. In addition, the draft international convention to enhance protection from cyber crime and terrorism, which was developed as a follow-up to a conference hosted by Stanford University, United States, in 1999 and the draft ITU toolkit on cybercrime legislation, which was developed by representatives of the American Bar Association and other experts.

Kluwer Law International, 1989).

[25] Regarding cybercrime legislation in European Union countries: Lorenzo Valeri and others, *Handbook of Legal Procedures of Computer Network Misuse in EU Countries* (Santa Monica, California, Rand Corporation, 2006).

[26] Council of Europe, *European Treaty Series*, No. 189. See also the "explanatory report" to the Additional Protocol.

[27] Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Moldova, Romania, Serbia, Slovenia, South Africa, Sweden, Switzerland, the former Yugoslav Republic of Macedonia and Ukraine.

[28] Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Romania, Serbia, Slovenia, the former Yugoslav Republic of Macedonia and Ukraine.

[29] Council of Europe, *Treaty Series*, No. 201.

[30] Albania, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Moldova, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, the former Yugoslav Republic of Macedonia, Turkey, Ukraine and United Kingdom.

[31] Albania, Denmark and Greece.

2. Territorialization

24. Theoretically, developments arising from technical standardization go far beyond the globalization of technology and services and could lead to the harmonization of national laws. However, as shown by the status of ratification of the Convention on Cybercrime and the negotiation of the Additional Protocol to the Convention, the principles of national law change much more slowly than technical developments do. This leads to a second development: approaches to territorialize the Internet.

25. Although the Internet may not recognize border controls, there are means to restrict access to certain information.[32] As a consequence, obligations of Internet service providers to block access to websites containing child pornography has come to the attention of national Governments and international organizations.[33] From a technical point of view, access providers are in general able to check whether the website that the user wants to access is on a blacklist and to block such access. The technical solutions range from a manipulation of the domain name system and the use of proxy servers, to hybrid solutions that combine various approaches.[34] The OpenNet Initiative reports that such kind of content control is practised by about two dozen countries.[35] Several European countries, including Italy, Norway, Sweden, Switzerland and the United Kingdom, as well as countries such as China, Iran (Islamic Republic of) and Thailand use such an approach. The European Union is also discussing the implementation of such obligations.[36] Concerns related to this approach focus on the fact that all technical solutions currently available can be circumvented and that there is the risk of being

---

[32] Jonathan Zittrain, "A history of online gatekeeping", *Harvard Journal of Law and Technology*, vol. 19, No. 2 (2006), p. 253.

[33] Regarding filter obligations and approaches, see: Ilaria Lonardo, "Italy: Service Provider's Duty to Block Content", *Computer Law Review International*, 2007, pp. 89 ff.; Ulrich Sieber and Malaika Nolde, *Sperrverfügungen im Internet: Nationale Rechtdurchsetzung im globalen Cyberspace?* (Berlin, Duncker and Humblot, 2008); W. Ph. Stol and others, *Filteren van kinderporno op internet: Een verkenning van technieken en reguleringen in binnen- en buitenland* (The Hague, Boom Juridische Uitgevers, WODC, 2008); Tom Edwards and Gareth Griffith, "Internet censorship and mandatory filtering", *NSW Parliamentary Library Research Service*, E-Brief 5/08, November 2008; Jonathan Zittrain and Benjamin Edelman, "Documentation of Internet filtering worldwide", October 2003, project available from http://cyber.law.harvard.edu/filtering.

[34] For an overview of the technical aspects see: Sieber and Nolde, *Sperrverfügungen im Internet*, pp. 50 ff.; Stol and others, *Filteren van kinderporno op internet*, pp. 10 ff.; Andreas Pfitzmann, Stefan Köpsell and Thomas Kriegelstein, *Sperrverfügungen gegen Access-Provider: Technisches Gutachten*, Technical University of Dresden, available from www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; Richard Clayton, Steven J. Murdoch and Robert N. M. Watson, "Ignoring the Great Firewall of China", paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, June 2006; Lori Brown Ayre, *Internet Filtering Options Analysis: An Interim Report*, prepared for the InfoPeople Project, May 2001.

[35] Miklós Haraszti, "Preface", in *Governing the Internet: Freedom and Regulation in the OSCE Region*, C. Möller and A. Amouroux, eds. (Vienna, Organization for Security and Cooperation in Europe, 2007), pp. 5-6.

[36] Commission of the European Communities, "Proposal for a Council framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing framework decision 2004/68/JHA", document COM(2009) 135, Brussels, 25 March 2009.

overzealous in blocking access to information on the Internet.[37] The importance of protecting fundamental rights has been pointed out by the Council of Europe in its Committee of Ministers recommendation on measures to promote respect for freedom of expression and information with regard to Internet filters.

D. Organized crime

26. While computer-related crimes are in general committed by individuals, organized criminal groups are active as well. This development is especially relevant as it introduces the possibility for the application of instruments designed to address organized crime, such as the United Nations Convention against Transnational Organized Crime.[38]

27. In discussing cybercrime and organized crime, it is necessary to distinguish between two main categories of involvement by organized criminal groups: the use of information technology by traditional organized criminal groups and organized crime groups focusing on committing cybercrime.[39]

28. Traditional organized criminal groups without a background in Internet-related criminal activities are using information technology to coordinate activities and enhance the commission of crimes.[40] In such cases, information technology is used to improve the efficiency of the organized criminal group in its traditional field of activity. This includes the shift to electronic communications, which for example enables the organized criminal groups to make use of encryption technology and to communicate anonymously. In addition, the Internet can be used to open new markets, for, as the United Kingdom's Organised Crime Task Force has found, the Internet has provided a new and much larger marketplace for those involved in the sale of counterfeit and pirated goods.[41]

29. Reports point to a trend of traditional organized criminal groups getting involved with new forms of criminal activities in the area of high-tech crimes.[42] This includes software piracy and other forms of copyright infringement.[43] But

---

[37] For more on Internet blocking and balancing fundamental freedoms, see Cormac Callanan and others, *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Dublin, Aconite Internet Solutions, October 2009), chaps. 6 and 7.

[38] United Nations, *Treaty Series*, vol. 2225, No. 39574.

[39] Kim-Kwang Raymond Choo, "Organised crime groups in cyberspace: a typology", *Trends in Organized Crime*, vol. 11, No. 3 (September 2008), pp. 270-295. In this article, Choo suggests that there are three categories of organized criminal groups that exploit information technologies to infringe controls.

[40] Ibid., p. 273; Eoghan Casey, *Digital Evidence and Computer Crime: Forenisc Science, Computers, and the Internet*, 2nd ed. (London, Academic Press, 2004), p. 9.

[41] United Kingdom, Organised Crime Task Force, *Annual Report and Threat Assessment 2007: Organised Crime in Northern Ireland* (2007), p. 34. Available from www.octf.gov.uk.

[42] United Kingdom, Serious Organised Crime Agency, *The United Kingdom Threat Assessment of Organised Crime: 2009/10*, p. 10. Available from www.soca.gov.uk.

[43] Canada, Canadian Security Intelligence Service, "Transnational criminal activity: a global context", *Perpectives*, 17 August 2000, available from www.csis-scrs.gc.ca/pblctns/prspctvs/200007-eng.asp; Choo, "Organised crime groups", p. 273 (see footnote 40).

other areas of cybercrime, such as child pornography[44] and identity-related crime, are also often linked to organized crime. With regard to the implementation of the Organized Crime Convention, the following special features and organized cybercrime groups need to be taken into consideration:

(a) Cybercrime groups tend to have a looser and more flexible structure, which allows the incorporation of members in the group for a limited period of time;[45]

(b) Cybercrime groups are often much smaller than traditional organized criminal groups;[46]

(c) Often the members of the groups communicate exclusively in electronic form, never meeting in person.

III. Response to cybercrime

30. International and regional organizations, national governments, law enforcement agencies and non-governmental organizations are addressing cybercrime in various ways, including through legislative, law enforcement and capacity-building means.

A. Legislation

31. Currently, cybercrime legislation is mainly being developed at the national and regional levels. Unlike the technical standards used for data transfer processes, which are the same in all parts of the world, so far no efforts have been made at the global level to harmonize legislation on cybercrime.

1. Limited reach of existing instruments

32. The global impact of the regional approaches that have been adopted by the Commonwealth, the Economic Community of West African States (ECOWAS), the European Union and the Council of Europe — is limited as the approaches adopted are applicable only to the States members of the respective organizations. Currently, the instrument with the broadest reach is the Convention on Cybercrime, which is recognized as important in the fight against cybercrime and is supported by different international organizations. In addition, the Convention, pursuant to its article 37,

---

[44] Choo, "Organised crime groups", p. 281; European Police Office (Europol), "Child abuse in relation to trafficking in human beings", Serious Crime Overview, January 2008, p. 2; *Organised Crime Situation Report 2005*, p. 8; John Carr, *Child Abuse, Child Pornography and the Internet* (London, NCH, The Children's Charity, 2004), p. 17; Canada, Criminal Intelligence Service Canada, *Annual Report on Organized Crime in Canada 2007* (Ottawa, 2007), p. 4; "Annual report on organized crime in Greece for the year 2004", *Trends in Organized Crime*, vol. 9, No. 2 (2005), p. 5; United Nations, Commission on Human Rights, Report of the Special Rapporteur on the sale of children, child prostitution and child pornography (E/CN.4/2005/78), p. 8.

[45] Choo, "Organised crime groups" p. 273 (see footnote 40).

[46] Susan W. Brenner, "Organized cybercrime? How cybercrime may affect the structure of criminal relationships", North Carolina Journal of Law and Technology, No. 4 (2002), p. 27.

may also be acceded to by any State that is not a member of the Council. Four non-member States (Canada, Japan, South Africa and the United States) were involved in the negotiation of the Convention, three of which (Canada, Japan and the United States) are closely connected to the Council by their observer status. As at December 2009, 46[47] States (among them the four non-members that participated in the negotiation) had signed the Convention; 26 States and 1 non-member of the Council have ratified the Convention to date.[48]

33. The impact of the Convention on Cybercrime cannot be measured solely by the number of States that have signed or ratified the Convention. Argentina, Botswana, Egypt, Nigeria, Pakistan and the Philippines, for example, have modelled parts of their legislation on the Convention without formally acceding to it. But, compared to global standards, the number and speed of signature and ratification certainly remains an issue. In the nine years since the first 30 States signed the Convention on 23 November 2001, only 16 additional States have become signatories. Since 2001, no non-member of the Council of Europe has acceded to the Convention, although five States (Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines) have been invited to do so. The pace of ratification has been similarly slow, with two States (Albania and Croatia) ratifying the Convention in 2002, two (Estonia and Hungary) in 2003, four (Lithuania, Romania, Slovenia and the former Yugoslav Republic of Macedonia) in 2004, three (Bulgaria, Cyprus and Denmark) in 2005, seven (Armenia, Bosnia and Herzegovina, France, the Netherlands, Norway, Ukraine and the United States) in 2006, three (Finland, Iceland and Latvia) in 2007, two (Italy and Slovakia) in 2008 and three (Germany, Republic of Moldova and Serbia) in 2009. As the Convention, in addition to being ratified, in general needs to be implemented, the efficiency of the instrument depends on the full adaptation of national law by those States that have ratified the Convention. Moreover, proof of full adaptation is needed.

2. Global debate

34. Another aspect of the role of regional frameworks as instruments for a global harmonization is the ability of non-members to participate. Despite the transnational dimension of cybercrime, the impact in the different regions of the world is different. This is especially relevant for developing countries.[49] The regional approaches mentioned in paragraph 32 above do not offer a possibility for a broad involvement of non-members. While the Convention on Cybercrime is currently the

---

[47] Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Moldova, Romania, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Ukraine, United Kingdom and United States.

[48] Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Republic of Moldova, Romania, Serbia, Slovakia, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine and United States.

[49] See, for example, the report of the Organization for Economic Cooperation and Development, *Spam Issues in Developing Countries* (Paris, OECD, 2005), p. 4. Available from http://www.oecd.org/dataoecd/5/47/34935342.pdf); and *Understanding Cybercrime: A Guide*, p. 15 (see footnote 2).

instrument with the broadest membership, even it limits the possibility of non-members to participate. In article 37 of the Convention, it is stipulated that accession requires States to consult with and obtain the unanimous consent of the contracting States to the Convention. In addition, participation in the debate about possible future amendments is limited to parties of the Convention (art. 44).

35. Experience has shown that States are generally reluctant to ratify or accede to conventions that they have not contributed to developing and negotiating. This has been true regardless of the topic of the conventions.

36. At all four regional preparatory meetings for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, calls were made for the development of an international convention on cybercrime.

37. Another such call was made at the meetings of the Heads of National Law Enforcement Agencies, Africa, the Near and Middle East and Europe, at which discussions were held on the Internet, electronic evidence gathering, legislation etc. At meetings held in other regions, participants concluded that law enforcement agencies and judiciaries were poorly prepared and had insufficient capacity to address developments in cybercrime and to gather and use evidence from cybertechnologies in the preparation of prosecutions. There was universal agreement that national laws were not keeping pace and that amendments were needed to support the investigation, prosecution and conviction of offenders on the basis of evidence captured through cybertechnology. There is an urgent need for common rules and cooperation between States so that authorities can act effectively across jurisdictions to bring offenders to justice. Calls for an international instrument have also come from academia.[50]

3. Response to recent trends

38. Cybercrime is constantly changing. When regional approaches such as the Commonwealth model law on computer and computer-related crime and the Convention on Cybercrime were being developed, large-scale "botnet attacks", "phishing" and terrorist use of the Internet were either not known or did not play as important a role as they do today. As a consequence, they are not addressed by specific provisions. At the regional preparatory meetings for the Twelfth Congress the demand for addressing those new phenomena was addressed, especially terrorist use of the Internet ranging from propaganda, communication and financing of terrorism by means of Internet-related payment services to the collection of information about a potential target. The phenomena as well as possible legal responses have been addressed on several occasions by the Counter-Terrorism Implementation Task Force.[51]

39. While, with regard to substantive criminal law, such phenomena can often be covered by applying provisions on system interference or computer-related forgery,

---

[50] Joachim Vogel, "Towards a global convention against cybercrime", paper presented at the First World Conference of Penal Law, Guadalajara, Mexico, 19-23 November 2007; Stein Schjølberg and Solange Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and Security in Cyberspace* (Oslo, E-dit, 2009).

[51] See, for example: Counter-Terrorism Implementation Task Force, "Report of the Working Group on Countering the Use of Internet for Terrorist Purposes", February 2009. Available from www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf.

the application of procedural instruments contained in existing regional instruments is far more difficult, especially since the technologies and the services offered through the Internet (social networks, for example) have significantly changed. The interception of voice-over-Internet-Protocol communication, the admissibility of digital evidence in criminal proceedings, procedures for investigating cases involving encryption technology or means of anonymous communication are urgent issues that are not, however, being addressed at the regional level and only in some cases are they being addressed at the national level.[52]

40. Addressing those issues is important, as traditional investigative instruments often fail when it comes to cybercrime investigations. One example is the interception of communications. In recent decades, States have developed investigation instruments, such as wiretapping, that have enabled them to intercept mobile and non-mobile telephone communications. Traditional telephone calls are usually intercepted through telecommunication providers. Applying the same principle to Voice-over-Internet-Protocol communication, law enforcement agencies would need to interact with Voice-over-Internet-Protocol service providers. However, if their service is based on peer-to-peer technology,[53] service providers may generally be unable to intercept communications, as the relevant data is transferred directly between the communicating partners.[54] Therefore, new techniques, in addition to the related legal instruments, might be needed.

41. The ability to carry out sophisticated investigations is not only relevant to new offences but also to more traditional forms of cybercrime, such as child pornography. Since the mid-1990s, distributors and consumers of child pornography have had access to network services that are used ever more intensively.[55] The Internet has become the primary medium for exchanging child pornography. The problems related to detecting and investigating child pornography cases have been recognized since the 1990s; they continue to exist in large part because offenders can make use of sophisticated technology to hinder investigations. According to one study, for example, 6 per cent of people caught with child pornography used encryption technology, 17 per cent used password-protected software, 3 per cent used evidence-eliminating software and 2 per cent used remote storage systems.[56] In addition, a shift with regard to technology has been observed: while in the early days of the Internet the exchange through traditional channels such as Internet relay

---

[52] For an overview of different national approaches addressing the issues see: *Understanding Cybercrime: A Guide*, chap. 6 (see footnote 2).

[53] Peer-to-peer technology enables direct connectivity between participants in networks instead of obliging users to communicate using conventional centralized server-based structures.

[54] Regarding the interception of Voice-over-Internet-Protocol communications by law enforcement agencies, see Steven Bellovin and others, "Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP", 13 June 2006, available from www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf; Matthew Simon and Jill Slay, "Voice over IP: forensic computing implications", paper presented at the 4th Australian Digital Forensics Conference, Perth, Australia, December 2006.

[55] United States, House of Representatives, "Sexual exploitation of children over the Internet" (2007), 109th Congress, p. 9.

[56] Janis Wolak, David Finkelhor and Kimberly J. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crime: Findings From the National Juvenile Online Victimization Study* (Alexandria, Virginia, National Center for Missing and Exploited Children, 2005), p. 9.

chat dominated, recently child pornography has been exchanged through other technology, such as peer-to-peer networks.[57]

B. Law enforcement

42. In addition to relying on legal instruments, law enforcement depends to a large degree on the availability of investigation tools like forensic software (to collect evidence, to key-log and to decrypt or recover deleted files) and investigation management software or databases (e.g. with hash values from known child pornography images). In recent years, several of those tools have been and continue to be developed.[58] For example, a research project entitled "Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis" is being carried out at University College Dublin (information available from http://cci.ucd.ie/?q=node/33) and in December 2009 a new technology for tracking child pornography called PhotoDNA was introduced in the United States. One of the main issues related to the development of such tools remains the need for developers to coordinate efforts so as to avoid duplication. Similarly, the efforts of networks of contact points (such as those of the Group of Eight and INTERPOL, and the network linked to the Convention on Cybercrime) also need to be coordinated.

C. Capacity-building

43. Cybercrime is an issue not only for developed countries, but also for developing countries. According to the Development Gateway Foundation, in 2005 there were more Internet users in developing countries than in industrial nations.[59] The fact that ECOWAS recently adopted a directive on cybercrime and that the East African Community has presented a draft framework for cyberlaws are positive signs. Further support could help law enforcement agencies to prepare for offences that might be committed when broadband access becomes available to more users in the developing world. The General Assembly, in its resolution 64/179, entitled "Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity", drew attention to the emerging policy issues identified by the Secretary-General (A/64/123) of piracy, cybercrime, sexual exploitation of children and urban crime, and invited UNODC to explore, within its mandate, ways and means of addressing those issues.

---

[57] United States, General Accountability Office, *File-Sharing Programs, Child Pornography is Readily Accessible over Peer-to-Peer Networks*, testimony before the Committee on Government Reform, House of representatives, GAO Report GAO-03-537T (Washington, D.C., March 2003); Gretchen Ruethling, "27 charged in international online child pornography ring", *New York Times*, 16 March 2006; Choo, "Organised crime groups", p. 282 (see footnote 40); United Kingdom, Stockport Safeguarding Children Board, *Safeguarding Children in Stockport: Policy and Practice Handbook* (May 2008), p. 299, available at http://www.safeguardingchildreninstockport.org.uk/documents/Section%2000%20-%20Preface%20and%20contents.pdf.

[58] See, for example, the research project entitled "Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis" being carried out at University College Dublin (information available from htt://cci.ucd.ie/?q=node/33).

[59] Information available from http://topics.developmentgateway.org/special/informationsociety.

D. Training

44. As investigating cybercrime and prosecuting those involved in committing it entails unique challenges, it is important to provide training to law enforcement officers, prosecutors and judges. As emphasized at a UNODC expert group meeting on cybercrime, held in Vienna on 6 and 7 October 2009, most international and regional organizations dealing with the issue have taken steps to train experts involved in cybercrime investigation and develop training material.[60]

IV. Conclusions and recommendations

45. Investigating cybercrime and prosecuting cybercriminals is challenging for all institutions involved. Taking into account the complexity of the issue and the constant technical development, sustained and ever-expanding training for all authorities involved remains a key issue. The discussion held at the 2009 meeting of the UNODC expert group on cybercrime showed that institutionalized capacity-building and long-term sustainability are two key factors for measuring the success of future initiatives.

46. In order to eliminate safe havens and improve international cooperation, attention should be paid to closing gaps in existing legislation and to promoting consistency, coherence and compatibility of laws. Taking into account the importance of harmonizing legislation and of building on the outcomes of the preparatory meetings for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, the development of a global convention against cybercrime should be given careful and favourable consideration.

47. In the meantime, UNODC, as a standard-setter in crime prevention and criminal justice matters, will offer a multilateral platform with a focus on developing countries. It will continue to adopt a comprehensive, partnership-based and multidisciplinary approach by pooling its already proven legal, law enforcement and technical expertise to counter criminal activities, together with the specific and well-developed expertise of those key partners already involved in countering cybercrime. UNODC will aim to partner with and bring together the tools and experts, including from the private sector (in particular Internet service providers), to tackle the problem in a given country or region. Priority will be accorded to the provision of technical assistance to Member States in need, with a view to addressing the lack of capacity and expertise, and to ensuring long-term sustainability in dealing with computer-related crime.

---

[60] For example, the Asia-Pacific Economic Cooperation has organized several training events on cybercrime, including legislation on cybercrime; the Commonwealth has organized legal and technical training sessions; the Council of Europe has contributed to training events in various parts of the world and developed specific training material for judges; the European Union has supported the development of cybercrime training sessions and materials for law enforcement agencies of its member States and organized several training sessions inside and outside Europe; INTERPOL has organized several training sessions for law enforcement agencies and developed training material; ITU has developed training material on cybercrime available in all United Nations languages, provided general training at several regional events and provided specific training for judges.

48. Specifically, UNODC will aim to do the following: assist Member States in adopting legislation for effectively investigating computer-related crimes and prosecuting offenders; build the operational and technical knowledge of judges, prosecutors and law enforcement officers on issues pertaining to cybercrime, through training, the adaptation/development of training materials on investigation and prosecution of computer-related crime etc.; train law enforcement authorities to effectively use international cooperation mechanisms to combat cybercrime; raise the awareness of civil society and create momentum among decision makers to coalesce efforts to prevent and address cybercrime; and identify and disseminate good practices and promote public-private partnerships in preventing and combating cybercrime.