United Nations E/CN.15/2013/24

Economic and Social Council

Distr.: General
5 March 2013

Original: English

Commission on Crime Prevention and Criminal Justice
Twenty-second session
Vienna, 22-26 April 2013
Item 7 of the provisional agenda*
World crime trends and emerging issues and responses in the field of crime prevention and criminal justice

Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building

Report of the Secretary-General

Summary

The present report has been prepared pursuant to Commission on Crime Prevention and Criminal Justice resolution 20/7, entitled "Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building". It contains a summary of the activities of the United Nations Office on Drugs and Crime (UNODC) with regard to providing technical and capacity-building assistance to Member States, as well as an overview of the activities carried out by UNODC to support the Expert Group to Conduct a Comprehensive Study on Cybercrime and the executive summary of the draft study on cybercrime.

* E/CN.15/2013/1.

V.13-80773 (E) 110313 120313

I. Introduction

1. The present report was prepared pursuant to Commission on Crime Prevention and Criminal Justice resolution 20/7, entitled "Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building".

2. In that resolution, the Commission requested the United Nations Office on Drugs and Crime (UNODC), in cooperation with Member States, relevant international and regional organizations and, as appropriate, the private sector, to continue to provide, upon request, technical assistance and training to States, based on national needs, especially with regard to the prevention, detection, investigation and prosecution of cybercrime in all its forms, without prejudice to the work and outcomes of the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime and responses to it by Member States, the international community and the private sector.

3. Furthermore, the Commission took note of the outcome of the first meeting of the Expert Group (see E/CN.15/2011/19) and requested UNODC to strengthen cooperation with Member States; relevant organizations, such as the International Criminal Police Organization (INTERPOL), the European Police Office, the International Telecommunication Union (ITU), the European Commission, the Council of Europe, the Shanghai Cooperation Organization and the Commonwealth of Independent States; and the private sector, including computer companies and Internet service providers, on combating cybercrime.

II. Work of the United Nations Office on Drugs and Crime, in cooperation with Member States, international and regional organizations, and the private sector to provide technical assistance and training to States

4. In 2012, UNODC finalized a Global Programme on Cybercrime, which adopted a holistic approach focusing on: (a) delivery of training for law enforcement and criminal justice practitioners on techniques for investigating and criminal justice approaches to cybercrime; (b) prevention and raising awareness of cybercrime; (c) enhanced national, regional and international cooperation in addressing cybercrime; and (d) data collection, research and analysis on the links between organized crime and cybercrime. In the framework of that programme, UNODC will promote sustainable and long-term capacity-building, including through training sessions, in cooperation with a range of partners, including ITU, the private sector and academic experts.

5. All of the activities in the Global Programme on Cybercrime are designed to lead to an increase in long-term, sustainable national capacities for preventing and combating cybercrime. Activities under the Programme will be implemented primarily by UNODC as the executing agency, with additional support from ITU and other relevant partners, where required and according to subject matter area, Government request and relevant mandate.

6. In May 2011, UNODC signed a memorandum of understanding with ITU for the purpose of cooperation in the delivery of technical assistance in the area of

cybercrime and cybersecurity, within the respective mandates of each organization.[1] Pursuant to that memorandum, UNODC has worked with ITU in the delivery of technical assistance upon request from States. In this context, UNODC focuses on addressing the crime prevention and criminal justice aspects of cybercrime, while ITU works to enhance cybersecurity, including through the protection of critical infrastructure from computer-based attacks.

7. In its resolution 2011/33, entitled "Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children", the Economic and Social Council requested UNODC to carry out a study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children, taking into account relevant data collected by the Expert Group. In that resolution, the Council also requested UNODC to design and carry out an assessment of the needs of States for training in the investigation of offences against children committed by using new information and communications technologies and, on the basis of the results of that survey, to design a training and technical assistance programme to assist Member States in combating such offences more effectively.

8. In 2011 and in the first half of 2012, UNODC commenced a literature review for the study on the effects of new information technologies on the abuse and exploitation of children, and it took preparatory steps with regard to the assessment of training needs. In accordance with Economic and Social Council resolution 2011/33, a report on the implementation of that resolution, including activities related to the study, will be presented to the Commission for consideration at its twenty-third session, in 2014.

9. In April and May 2012, UNODC organized workshops in Nairobi for 10 countries in East and Southern Africa; in Beirut for 12 countries in West Asia; and in Bangkok for 11 countries in South-East and South Asia. The workshops provided an opportunity to obtain information on the technical assistance needs of those countries in the area of cybercrime. The workshops showed that there was: (a) an identified need for basic training for policymakers and decision makers in order to increase the priority placed on cybercrime issues; (b) a need for further development of mechanisms for both formal and informal international cooperation between law enforcement officers and prosecutors; (c) a need for improved access to and training on forensics software and hardware for conducting cybercrime investigations; and (d) a need for the promotion of public-private partnerships in order to strengthen measures to prevent cybercrime. On the basis of the outcomes of the workshops, UNODC is presently exploring options for the delivery of technical assistance within the framework of the Global Programme on Cybercrime and in conjunction with relevant partners, including ITU, and for countries in East and Southern Africa.

10. Representatives of UNODC attended meetings with major global electronic service providers to continue progress towards private sector support and engagement with the Global Programme on Cybercrime. The Programme envisions close cooperation with private sector partners and relevant intergovernmental organizations to provide collaborative support for capacity-building programmes. The Programme has been designed to facilitate working relations between law

[1] See www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf.

enforcement and local offices of key global electronic service providers, including the delivery of presentations to specialized cybercrime law enforcement officers by global service providers on corporate procedures and due legal process requirements and the facilitation of the streaming of strategic threat information from key global cybersecurity providers to law enforcement.

11. In February 2012, an initial assessment mission was undertaken to Panama, at the request of the Government, for the purpose of further developing national capacity to counter cybercrime. Organized jointly by UNODC headquarters and the Regional Office for Central America and the Caribbean, the mission worked with a cross-departmental Government working group to review and revise the legislative framework for cybercrime. The working group, involving national authorities and opinion leaders, as well as private sector entities, was established to work on cybercrime legislation for Panama. Consultations were held to agree on a broad and comprehensive approach to countering cybercrime in that country. The Panamanian authorities also expressed interest in the ITU-UNODC cooperative approach and the support that they might receive in strengthening the defence of critical infrastructure of Panama.

12. In addition, with a view to further strengthening cooperation and raising awareness of cybercrime, in 2012 UNODC conducted a workshop in the Islamic Republic of Iran, upon request, to deliver training sessions to 80 law enforcement and Ministry of Justice officials on cybercrime. Meetings were also held with the local office of INTERPOL, the cybercrime police, and the judiciary in order to enhance global cooperation against cybercrime.

III. Activities of the United Nations Office on Drugs and Crime to strengthen cooperation with Member States, intergovernmental organizations and the private sector

13. To further enhance cooperation against cybercrime at all levels, UNODC has continued to participate as an observer in the consultations of the Council of Europe Cybercrime Convention Committee, in the framework of the Council of Europe Convention on Cybercrime, and in its annual “Octopus” conference.

14. UNODC also participated as a partner in the Commonwealth Cybercrime Initiative, in which UNODC sought ways to improve cooperation between UNODC and Initiative partners. UNODC further participated as an observer in the European Cybercrime Training and Education Group and cooperated with the Organization for Security and Cooperation in Europe in the context of its annual meeting of police experts.

IV. Activities of the United Nations Office on Drugs and Crime to support the Expert Group to Conduct a Comprehensive Study on Cybercrime[a]

15. The first meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime was held in Vienna from 17 to 21 January 2011. At that meeting, the Expert Group reviewed and adopted a collection of topics and a methodology for the study (see E/CN.15/2011/19). The methodology provided for the distribution of a questionnaire to Member States, intergovernmental organizations and representatives from the private sector and academic institutions. Information gathering was conducted by UNODC, in accordance with the agreed methodology, from February 2012 to July 2012.[2]

16. A draft questionnaire was sent for comment to all Member States in June 2012. Following receipt of comments, the questionnaire was finalized by UNODC and disseminated through the use of a web-based data collection portal. In order to confirm with Member States that aspects of the information gathered and analysed were correct, UNODC sent a summary to each State of its cybercrime legislative provisions for comment and correction where necessary. In November 2012, UNODC consulted with experts nominated by each regional group regarding preliminary analysis of results received from questionnaires completed by Member States. On the basis of responses to the questionnaire received from Member States, the private sector and academic and intergovernmental organizations, UNODC prepared a draft study for consideration by the expert group.

17. The second meeting of the Expert Group was held from 25 to 28 February 2013.[3] At that meeting, the Expert Group took note of and considered the comprehensive study on cybercrime as prepared by UNODC under the auspices of the Expert Group. The Expert Group noted that its deliberations, as well as the study, reflected a compilation of views and different approaches taken by States to preventing and combating the phenomenon of cybercrime. In discussions concerning the cybercrime study, it was noted that there was broad support for capacity-building and technical assistance, and for the role of UNODC in that regard. Diverse views were expressed regarding the content, findings and options presented in the study. The Expert Group discussed the way forward and recommended that the study be further considered by the Commission at its twenty-second session.

18. The executive summary of the comprehensive study, provided below, was prepared by UNODC, as it had been tasked with doing by the Expert Group. The findings and options contained in the study and the executive summary were

---

[a] The text of section IV was originally issued in an unedited background document (UNODC/CCPCJ/EG.4/2013/2); in the present report it has been edited in accordance with the established standards of the Secretariat.

[2] Information was received from 69 Member States, with regional distribution as follows: Africa (11), Americas (13), Asia (19), Europe (24) and Oceania (2). Information was received from 40 private sector organizations, 17 academic organizations and 11 intergovernmental organizations. Over 500 open-source documents were also reviewed by the Secretariat.

[3] The outcome of the meeting is contained in UNODC/CCPCJ/EG.4/2013/3.

prepared by UNODC on the basis of empirical information provided and are not intended to constitute recommendations.[4]

A. Executive summary of the comprehensive study of the problem of cybercrime prepared by the United Nations Office on Drugs and Crime

1. Global connectivity and cybercrime

19. In 2011, at least 2.3 billion people, the equivalent of approximately one third of the world's total population, had access to the Internet. Over 60 per cent of all Internet users were in developing countries, with 45 per cent of all Internet users below the age of 25 years. By 2017, it is estimated that the number of mobile broadband subscriptions will approach 70 per cent of the world's total population. By 2020, the number of networked devices (the "Internet of things") will outnumber people by six to one, transforming current conceptions of the Internet. In the hyperconnected world of tomorrow, it will become hard to imagine a "computer crime", and perhaps any crime, that does not involve electronic evidence linked with Internet protocol connectivity.

20. Definitions of cybercrime depend mostly upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term "cybercrime") do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term. Certain definitions are required for core acts of cybercrime. However, a definition of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which are better focused on electronic evidence of any crime, rather than a broad, artificial "cybercrime" construct.

2. The global cybercrime picture

21. In many countries, the explosion in global connectivity has come at a time of economic and demographic transformation, with rising income disparities, tightened private sector spending and reduced financial liquidity. At the global level, law enforcement respondents to the study perceived increasing levels of cybercrime, as both individuals and organized criminal groups exploit new criminal opportunities, driven by profit and personal gain. Upwards of 80 per cent of acts of cybercrime are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale and "cashing out" of financial information. Cybercrime perpetrators no longer require complex skills or techniques. In the developing country context in particular, subcultures of young men engaged in computer-related financial fraud have emerged, many of whom begin involvement in cybercrime in their late teenage years.

[4] The full study is made available in English only, as referenced in E/CN/15/2013/CRP.5.

22. Globally, acts of cybercrime are broadly distributed among financially driven acts and computer-content-related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems. Perceptions of relative risk and threat vary, however, between Governments and private sector enterprises. Currently, police-recorded crime statistics do not represent a sound basis for cross-national comparisons, although such statistics are often important for policymaking at the national level. Two thirds of countries view their systems of police statistics as insufficient for recording cybercrime. Police-recorded cybercrime rates are associated with levels of country development and specialized police capacity, rather than underlying crime rates.

23. Victimization surveys represent a more sound basis for comparison. These demonstrate that the rate of individual cybercrime victimization is significantly higher than for "conventional" forms of crime. Victimization rates for online credit card fraud, identity theft, responding to a "phishing" attempt and experiencing unauthorized access to an e-mail account vary between 1 and 17 per cent of the online population for 21 countries around the world, compared with typical burglary, robbery and car theft rates of under 5 per cent for these same countries. Cybercrime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen prevention efforts in these countries.

24. Private sector enterprises in Europe report similar victimization rates — between 2 and 16 per cent — for acts such as data breach due to intrusion or "phishing". Criminal tools of choice for these crimes, such as botnets, have global reach. More than one million unique Internet protocol addresses globally functioned as botnet command and control servers in 2011. Internet content also represented a significant concern for Governments. Material targeted for removal included child pornography and hate speech, but also content related to defamation and Government criticism, raising human rights law concerns in some cases. Almost 24 per cent of total global Internet traffic is estimated to infringe copyright, with downloads of shared peer-to-peer (P2P) material particularly high in countries in Africa, South America and Western and South Asia.

3. Cybercrime legislation

25. Legal measures play a key role in the prevention and combating of cybercrime. These are required in all areas, including criminalization, procedural powers, jurisdiction, international cooperation and Internet service provider responsibility and liability. At the national level, both existing and new (or planned) cybercrime laws most often concern criminalization, indicating a predominant focus on establishing specialized offences for core acts of cybercrime. Countries increasingly recognize, however, the need for legislation in other areas. Compared with existing laws, new or planned cybercrime laws more frequently address investigative measures, jurisdiction, electronic evidence and international cooperation. Globally, less than half of responding countries perceived their criminal and procedural law frameworks to be sufficient, although this masks large regional differences. While more than two thirds of countries in Europe reported sufficient legislation, the reverse was the case in Africa, the Americas, Asia and Oceania, where more than two thirds of countries viewed laws as only partly sufficient or not sufficient at all. Only one half of the countries reporting that laws were insufficient also indicated

new or planned laws, thus highlighting an urgent need for legislative strengthening in these regions.

26. The past decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and non-binding instruments. Five clusters can be identified, consisting of instruments developed in the context of or inspired by (a) the Council of Europe or the European Union, (b) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (c) intergovernmental African organizations, (d) the League of Arab States and (e) the United Nations. A significant amount of cross-fertilization exists between all instruments, including in particular concepts and approaches developed in the Council of Europe Convention on Cybercrime. Analysis of the articles of 19 multilateral instruments relevant to cybercrime shows common core provisions, but also significant divergence in substantive areas addressed.

27. Globally, 82 countries have signed and/or ratified a binding cybercrime instrument.[5] In addition to formal membership and implementation, multilateral cybercrime instruments have influenced national laws indirectly, through use as a model by non-States parties or via the influence of legislation of States parties on other countries. Membership of a multilateral cybercrime instrument corresponds with a perception of increased sufficiency of national criminal and procedural law, indicating that current multilateral provisions in these areas are generally considered effective. For the more than 40 countries that provided information, the Council of Europe Convention on Cybercrime was the most used multilateral instrument for the development of cybercrime legislation. Altogether, multilateral instruments from other "clusters" were used in around half as many countries.

28. Overall, one third of responding countries reported that their legislation was highly, or very highly, harmonized with countries viewed as important for the purposes of international cooperation. That varied regionally, however, with higher degrees of harmonization reported within the Americas and Europe. This may be due to the use, in some regions, of multilateral instruments, which are inherently designed to play a role in harmonization. Fragmentation at the international level, and diversity of national laws, with regard to acts of cybercrime that are criminalized, jurisdictional bases and mechanisms of cooperation may correlate with the existence of multiple cybercrime instruments with different thematic and geographic scope. Both instruments and regions presently reflect divergences derived from underlying legal and constitutional differences, including differing conceptions of rights and privacy.

4. Criminalization

29. Information on criminal laws relating to cybercrime was gathered through the study questionnaire, as well as by primary source analysis of available legislation

---

[5] One or more of the following: Council of Europe Convention on Cybercrime, Arab Convention on Combating Information Technology Offences (League of Arab States), Agreement on Cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information, or the Agreement in the Field of International Information Security (Shanghai Cooperation Organization).

collected by the Secretariat.[6] The study questionnaire referred to 14 acts commonly included in notions of cybercrime.[7] Responding countries described widespread criminalization of these 14 acts, with the primary exception of spam offences and, to some extent, offences concerning computer misuse tools, racism and xenophobia, and online solicitation or "grooming" of children. This reflects a certain baseline consensus on culpable cybercrime conduct. Countries reported few additional crimes other than those mentioned in the questionnaire. They mostly concerned computer content, including criminalization of obscene material, online gambling and online illicit markets, such as markets in drugs and persons. For the 14 acts, countries reported the use of cyber-specific offences for core acts of cybercrime against the confidentiality, integrity and accessibility of computer systems. For other forms of cybercrime, general (non-cyber-specific) offences were used more often. Both approaches were reported, however, for computer-related acts involving breach of privacy, fraud or forgery, and identity offences.

30. While high-level consensus exists regarding broad areas of criminalization, detailed analysis of the provisions in source legislation reveals divergent approaches. Offences involving illegal access to computer systems and data differ with respect to the object of the offence (data, system or information) and with regard to the criminalization of "mere" access or the requirement of further intent, such as to cause loss or damage. The requisite intent for an offence also differs in approaches to criminalization of interference with computer systems or data. Most countries require the interference to be intentional, while others include reckless interference. For interference with computer data, the conduct constituting interference ranges from damaging or deleting to altering, suppressing, inputting or transmitting data. Criminalization of illegal interception differs according to whether the offence is restricted to non-public data transmissions, and whether the crime is restricted to interception "by technical means". Not all countries criminalize computer misuse tools. For those that do, differences arise regarding whether the offence covers possession, dissemination or use of software (such as malware) and/or computer access codes (such as victim passwords). From the perspective of international cooperation, such differences may have an impact upon findings of dual criminality between countries.

31. Several countries have established cyber-specific offences for computer-related fraud, forgery and identity offences. Others extend general provisions on fraud or theft, or rely on offences covering constituent elements, such as illegal access, data interference and forgery in the case of identity offences. A number of content-related offences, particularly those concerning child pornography, show widespread criminalization. Differences arise, however,

---

[6] Primary source legislation was analysed for 97 Member States, including 56 that responded to the questionnaire, with regional distribution as follows: Africa (15), Americas (22), Asia (24), Europe (30) and Oceania (6).

[7] Illegal access to a computer system; illegal access, interception or acquisition of computer data; illegal data interference or system interference; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offences; computer-related copyright and trademark offences; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution or possession of child pornography; computer-related solicitation or "grooming" of children; and computer-related acts in support of terrorism offences.

regarding the definition of "child", limitations in relation to "visual" material or exclusion of simulated material, and acts covered. Although the vast majority of countries, for instance, cover production and distribution of child pornography, there is greater variation in the criminalization of possession and access. For computer-related copyright and trademark infringement, countries most often reported the application of general criminal offences for acts committed wilfully and on a commercial scale.

32. The increasing use of social media and user-generated Internet content has resulted in regulatory responses from Governments, including the use of criminal law, and in calls for respect for rights to freedom of expression. Responding countries reported varying boundaries to expression, including with respect to defamation, contempt, threats, incitement to hatred, insult to religious feelings, obscene material and undermining the State. The sociocultural element of some limitations is reflected not only in national law but also in multilateral instruments. Some regional cybercrime instruments, for example, contain broad offences regarding the violation of public morals, pornographic material and religious or family principles or values.

33. International human rights law acts as both a sword and a shield, requiring criminalization of (limited) extreme forms of expression while protecting other forms. Some prohibitions on freedom of expression, including incitement to genocide, hatred constituting incitement to discrimination, hostility or violence, incitement to terrorism and propaganda for war, are therefore required for States that are party to relevant international human rights instruments. For others, the "margin of appreciation" allows countries leeway in determining the boundaries of acceptable expression in line with their own cultures and legal traditions. Nonetheless, international human rights law will intervene at a certain point. For example, penal laws on defamation, disrespect for authority and insult that apply to online expression will face a high threshold of demonstrating that the measures are proportionate, appropriate and the least intrusive possible. Where content is illegal in one country, but legal to produce and disseminate in another, States will need to focus criminal justice responses on persons accessing content within the national jurisdiction, rather than on content produced outside of the country.

5. Law enforcement and investigations

34. Over 90 per cent of responding countries reported that acts of cybercrime most frequently came to the attention of law enforcement authorities through reports by individual or corporate victims. Responding countries estimate that the percentage of actual cybercrime victimization reported to the police ranged upwards from 1 per cent. One global private sector survey suggests that 80 per cent of individual victims of core acts of cybercrime do not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment and perceived reputational risks for corporations. Authorities in all regions of the world highlighted initiatives for increasing reporting, including online and hotline reporting systems, public awareness campaigns, private sector liaison and enhanced police outreach and information sharing. An incident-driven response to cybercrime must, however, be accompanied by medium- and long-term tactical investigations that focus on crime markets and the architects of criminal schemes. Law enforcement authorities in

developed countries are engaged in this area, including through undercover units targeting offenders on social networking sites, in chat rooms and on instant messaging and P2P services. Challenges in the investigation of cybercrime arise from criminal innovations by offenders, difficulties in accessing electronic evidence and internal resource, capacity and logistical limitations. Suspects frequently use anonymization and obfuscation technologies, and new techniques quickly make their way to a broad criminal audience through online crime markets.

35. Cybercrime investigations undertaken by law enforcement authorities require an amalgamation of traditional and new policing techniques. While some investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. The study questionnaire referred to 10 cybercrime investigative measures, ranging from generic search and seizure to specialized powers, such as preservation of computer data.[8] Countries most often reported the existence of general (non-cyber-specific) powers among all investigative measures. A number of countries also reported cyber-specific legislation, notably for ensuring expedited preservation of computer data and obtaining stored subscriber data. Many countries reported a lack of legal power for advanced measures, such as remote computer forensics. While traditional procedural powers can be extended to cyber-specific situations, in many cases such an approach can also lead to legal uncertainties and challenges to the lawfulness of evidence gathering, and thus to the admissibility of evidence. Overall, there is less core commonality among national approaches to investigative powers regarding cybercrime than there is with respect to the criminalization of many acts of cybercrime.

36. Irrespective of the legal form of investigative powers, all responding authorities use search and seizure for the physical appropriation of computer equipment and the capture of computer data. The majority of countries also use orders for obtaining stored computer data from Internet service providers. Outside of Europe, however, around one third of countries reported challenges in compelling third parties in an investigation to provide information. Around three quarters of countries use specialized investigative measures, such as real-time collection of data or expedited preservation of data. Use of investigative measures typically requires a minimum of initial evidence or a report of an act of cybercrime. More intrusive measures, such as those involving real-time collection of data or accessing of data content, often require higher thresholds, such as evidence of a serious act or demonstration of probable cause or reasonable grounds.

37. The interplay between law enforcement and Internet service providers is particularly complex. Service providers hold subscriber information, billing invoices, some connection logs, location information (such as cell tower data for mobile providers) and communication content, all of which can represent critical electronic evidence of an offence. National legal obligations and private sector data retention and disclosure policies vary widely by country, industry and type of data.

---

[8] Search for computer hardware or data; seizure of computer hardware or data; order for subscriber information; order for stored traffic data; order for stored content data; real-time collection of traffic data; real-time collection of content data; expedited preservation of computer data; use of remote forensic tools; and trans-border access to a computer system or data.

Countries most often reported using court orders to obtain evidence from service providers. In some cases, however, law enforcement may be able to obtain stored subscriber data, traffic data, and even content data, directly. In this respect, private sector organizations often reported not only a primary policy of requiring due legal process for data disclosure, but also voluntary compliance with direct law enforcement requests under some circumstances. Informal relationships between law enforcement and service providers, the existence of which was reported in more than half of all responding countries, assist the process of information exchange and trust-building. Responses indicated that there was a need to balance privacy and due process with disclosure of evidence in a timely manner, in order to ensure that the private sector did not become a "choke point" for investigations.

38. Cybercrime investigations invariably involve considerations of privacy under international human rights law. Human rights standards specify that laws must be sufficiently clear to give an adequate indication of the circumstances in which authorities are empowered to use an investigative measure, and that adequate and effective guarantees must exist against abuse. Countries reported the protection of privacy rights in national law, as well as a range of limits and safeguards with regard to investigations. When investigations are transnational, however, divergences in levels of protection give rise to unpredictability regarding foreign law enforcement access to data and potential jurisdictional gaps in privacy protection regimes.

39. Over 90 per cent of the countries that responded to the questionnaire had begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence. In developing countries, however, those structures were not well resourced and suffered from a capacity shortage. Countries with lower levels of development had significantly fewer specialized police, with around 0.2 per 100,000 Internet users nationally. The rate was two to five times higher in more developed countries. Seventy per cent of specialized law enforcement officers in less developed countries were reported to lack computer skills and equipment, and only half received training more than once a year. More than half of responding countries in Africa, and one third of countries in the Americas, reported that law enforcement resources for investigating cybercrime were insufficient. Globally, it is likely that the picture is even worse. The study received responses, for example, from only 20 per cent of the world's 50 least developed countries. All responding countries in Africa, and over 80 per cent of countries in the Americas and Asia and Oceania, reported requiring technical assistance. The most commonly cited area for which technical assistance was required was general cybercrime investigative techniques. Of those countries requiring assistance, 60 per cent indicated that this was needed by law enforcement agencies.

6. Electronic evidence and the criminal justice response

40. Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form. It can be stored or transient. It can exist in the form of computer files, transmissions, logs, metadata or network data. Digital forensics is concerned with recovering information, often volatile and easily contaminated, that may have evidential value. Forensics techniques include the creation of "bit-for-bit"

copies of stored and deleted information, “write-blocking” in order to ensure that the original information is not changed, and cryptographic file “hashes”, or digital signatures, that can demonstrate changes in information. Almost all countries reported some digital forensics capacity. Many responding countries, in all regions, however, noted insufficient numbers of forensic examiners, differences between capacity at the federal and state level, lack of forensics tools and backlogs due to overwhelming quantities of data for analysis. One half of countries reported that suspects made use of encryption, rendering access to this type of evidence difficult and time-consuming without the decryption key. In most countries, the task of analysing electronic evidence lay with law enforcement authorities. Prosecutors, however, must view and understand electronic evidence in order to build a case at trial. All countries in Africa and one third of countries in other regions reported insufficient resources for prosecutors to do so. Prosecution computer skills were typically lower than those of investigators. Globally, around 65 per cent of responding countries reported some form of prosecutorial cybercrime specialization. Just 10 per cent of countries reported specialized judicial services. The vast majority of cybercrime cases were handled by non-specialized judges, who, in 40 per cent of responding countries, did not receive any form of cybercrime-related training. Judicial training on cybercrime law, evidence collection and basic and advanced computer knowledge represented a particular priority.

41. Over 60 per cent of responding countries did not make a legal distinction between electronic evidence and physical evidence. While approaches varied, many countries considered that good practice, as it ensured fair admissibility alongside all other types of evidence. A number of countries outside of Europe did not admit electronic evidence at all, making the prosecution of cybercrime, and any other crime evidenced by electronic information, unfeasible. While countries did not, in general, have separate evidentiary rules for electronic evidence, a number of countries referred to principles such as the best evidence rule, the relevance of evidence, the hearsay rule, authenticity and integrity, all of which might have particular application to electronic evidence. Many countries highlighted challenges with regard to attribution of acts to a particular individual, and commented that this was often dependent upon circumstantial evidence.

42. The challenges facing both law enforcement investigators and prosecutors mean that “brought to justice” rates are low for cybercrime offenders. The number of suspects identified per police-recorded offence involving child pornography is comparable to that for other sex offences; however, suspects per recorded offence for acts such as illegal access and computer-related fraud or forgery are only around 25 per 100 offences. Very few countries were able to provide data on persons prosecuted or convicted. Calculations for cybercrime offences in one country, however, showed that the ratio of persons convicted to recorded offences was significantly lower than for other “conventional” crimes.

7. International cooperation

43. Countries responding to the study questionnaire reported that between 30 and 70 per cent of acts of cybercrime involved a transnational dimension, engaging issues of transnational investigations, sovereignty, jurisdiction, extraterritorial evidence and a requirement for international cooperation. A transnational dimension to a cybercrime offence arises when an element or substantial effect of the offence is

in another territory, or when part of the modus operandi of the offence is in another territory. International law provides for a number of bases of jurisdiction over such acts, including forms of territory-based jurisdiction and nationality-based jurisdiction. Some of these bases are also found in multilateral cybercrime instruments. While all countries in Europe consider that national laws provide a sufficient framework for the criminalization and prosecution of extraterritorial acts of cybercrime, from around one third to over one half of countries in other regions of the world report insufficient frameworks. In many countries, provisions reflect the idea that the "whole" offence need not take place within the country in order for territorial jurisdiction to be asserted. Territorial linkages can be made with reference to elements or effects of the act, or the location of computer systems or data utilized for the offence. When they arise, jurisdictional conflicts are typically resolved through formal and informal consultations between countries. Country responses do not reveal, at present, any need for additional forms of jurisdiction over a putative "cyberspace" dimension. Rather, forms of territoriality-based and nationality-based jurisdiction are almost always able to ensure a sufficient connection between acts of cybercrime and at least one State.

44. Forms of international cooperation include extradition, mutual legal assistance, mutual recognition of foreign judgments and informal police-to-police cooperation. Due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as the preservation of computer data. Use of traditional forms of cooperation for obtaining extraterritorial evidence in cybercrime cases predominates, with over 70 per cent of countries reporting using formal mutual legal assistance requests for that purpose. Within such formal cooperation, almost 60 per cent of requests use bilateral instruments as the legal basis. Multilateral instruments are used in 20 per cent of cases. Response times for formal mechanisms were reported to be on the order of months, for both extradition and mutual legal assistance requests, a timescale which presents challenges to the collection of volatile electronic evidence. Sixty per cent of countries in Africa, the Americas and Europe, and 20 per cent of countries in Asia and Oceania, reported the existence of channels for urgent requests. However, the impact of those channels on response times was unclear. Modes of informal cooperation were possible for around two thirds of reporting countries, although few countries had a policy for the use of such mechanisms. Initiatives for informal cooperation and for facilitating formal cooperation, such as 24/7 networks, offer important potential for faster response times. They are, however, underutilized, handling around 3 per cent of the total number of cybercrime cases encountered by law enforcement for the group of reporting countries.

45. Formal and informal modes of cooperation are designed to manage the process of State consent for the conduct of foreign law enforcement investigations that affect a State's sovereignty. Increasingly, however, investigators, knowingly or unknowingly, access extraterritorial data during evidence gathering without the consent of the State where the data is physically situated. This situation arises, in particular, as a result of cloud computing technologies that involve data storage at multiple data centres in different geographic locations. Data "location", while technically knowable, is becoming increasingly artificial, to the extent that even traditional mutual legal assistance requests will often be addressed to the country that is the seat of the service provider, rather than the country where the data centre

is physically located. Direct foreign law enforcement access to extraterritorial data could occur when investigators make use of an existing live connection from a suspect's device, or when investigators use lawfully obtained data access credentials. Law enforcement investigators may, on occasion, obtain data from extraterritorial service providers through an informal direct request, although service providers usually require due legal process. Relevant existing provisions on "transborder" access found in the Council of Europe Convention on Cybercrime and the Arab Convention on Combating Information Technology Offences do not adequately cover such situations, due to a focus on the "consent" of the person having lawful authority to disclose the data and on presumed knowledge of the location of the data at the time of access or receipt.

46. The current international cooperation picture risks the emergence of country clusters that have the necessary powers and procedures to cooperate among themselves, but that are restricted, with regard to all other countries, to "traditional" modes of international cooperation that take no account of the specificities of electronic evidence and the global nature of cybercrime. This is particularly the case for cooperation in investigative actions. A lack of a common approach, including within current multilateral cybercrime instruments, means that requests for action, such as for the expedited preservation of data outside of those countries with international obligations to ensure such a facility and to make it available upon request, may not be easily fulfilled. The inclusion of this power in the draft African Union cybersecurity convention may go some way towards closing this lacuna. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks and variance in cooperation safeguards represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters.

8. Cybercrime prevention

47. Crime prevention comprises strategies and measures that seek to reduce the risk of crimes occurring and mitigate potential harmful effects on individuals and society. Almost 40 per cent of responding countries reported the existence of national law or policy on cybercrime prevention. Initiatives were under preparation in a further 20 per cent of countries. Countries highlighted that good practices on cybercrime prevention included the promulgation of legislation, effective leadership, the development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base and cooperation among Government, communities and the private sector, as well as internationally. More than one half of countries reported the existence of cybercrime strategies. In many cases, cybercrime strategies were closely integrated into cybersecurity strategies. Around 70 per cent of all reported national strategies included components on awareness-raising, international cooperation and law enforcement capacity. For the purpose of coordination, law enforcement and prosecution agencies were most frequently reported as the lead cybercrime institutions.

48. Surveys, including in developing countries, demonstrate that most individual Internet users now take basic security precautions. The continued importance of

public awareness-raising campaigns, including those covering emerging threats and those targeted at specific audiences, such as children, was highlighted by responding Governments, private sector entities and academic institutions. User education is most effective when combined with systems that help users to achieve their goals in a secure manner. If user cost is higher than direct user benefit, individuals have little incentive to follow security measures. Private sector entities reported that user and employee awareness must be integrated into a holistic approach to security. Foundational principles and good practice referred to included accountability for acting on awareness, risk management policies and practices, board-level leadership and staff training. Two thirds of private sector respondents had conducted a cybercrime risk assessment, and most reported use of cybersecurity technology such as firewalls, digital evidence preservation, content identification, intrusion detection and system supervision and monitoring. Concern was expressed, however, that small and medium-sized companies either did not take sufficient steps to protect systems or incorrectly perceived that they would not be a target.

49. Regulatory frameworks have an important role to play in cybercrime prevention, both with respect to the private sector in general and service providers in particular. Nearly half of countries have passed data protection laws, which specify requirements for the protection and use of personal data. Some of these regimes include specific requirements for Internet service providers and other electronic communications providers. While data protection laws require personal data to be deleted when no longer required, some countries have made exceptions for the purposes of criminal investigations, requiring Internet service providers to store specific types of data for a period of time. Many developed countries also have rules requiring organizations to notify individuals and regulators of data breaches. Internet service providers typically have limited liability as "mere conduits" of data. Modification of transmitted content increases liability, as does actual or constructive knowledge of an illegal activity. Expeditious action after notification, on the other hand, reduces liability. While technical possibilities exist for the filtering of Internet content by service providers, restrictions on Internet access are subject to foreseeability and proportionality requirements under international human rights law protecting the rights to seek, receive and impart information.

50. Public-private partnerships are central to cybercrime prevention. Over half of all countries reported the existence of partnerships. These were created in equal numbers by informal agreement and by legal basis. Private sector entities were most often involved in partnerships, followed by academic institutions and international and regional organizations. Partnerships were mostly used for facilitating the exchange of information on threats and trends, but they were also used for prevention activities, and action in specific cases. Within the context of some public-private partnerships, private sector entities have taken proactive approaches to investigating and taking legal action against cybercrime operations. Such actions complement those of law enforcement and can help mitigate damage to victims. Academic institutions play a variety of roles in preventing cybercrime, including through delivery of education and training to professionals, law and policy development and work on technical standards and solution development. Universities house and facilitate cybercrime experts, some computer emergency response teams and specialized research centres.

B. Summary of key findings of the study

51. Key findings from the comprehensive study on cybercrime are:

(a) Fragmentation at the international level, and diversity of national cybercrime laws, may correlate with the existence of multiple instruments with different thematic and geographic scope. While instruments legitimately reflect sociocultural and regional differences, divergences in the extent of procedural powers and international cooperation provisions may lead to the emergence of country cooperation "clusters" that are not always well suited to the global nature of cybercrime;

(b) Reliance on traditional means of formal international cooperation in cybercrime matters is not currently able to offer the timely response needed for obtaining volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cybercrime, but also for all crimes in general;

(c) In a world of cloud computing and data centres, the role of evidence "location" needs to be reconceptualized, including with a view to obtaining consensus on issues concerning direct access to extraterritorial data by law enforcement authorities;

(d) Analysis of available national legal frameworks indicates insufficient harmonization of "core" cybercrime offences, investigative powers and admissibility of electronic evidence. International human rights law represents an important external reference point for criminalization and procedural provisions;

(e) Law enforcement authorities, prosecutors and the judiciary in developing countries require long-term, sustainable, comprehensive technical support and assistance for the investigation and combating of cybercrime;

(f) Cybercrime prevention activities in all countries require strengthening, through a holistic approach involving further awareness-raising, public-private partnerships and the integration of cybercrime strategies into a broader cybersecurity perspective.

C. Summary of options contained in the study

52. The options presented in the study prepared by UNODC were informed by the responses of countries to a question in the study questionnaire regarding options that could be considered to strengthen existing and to propose new national and international legal or other responses to cybercrime, as well as by the key findings. The study finds that such options may include one or more of the following:[9]

(a) The development of international model provisions on criminalization of core acts of cybercrime, with a view to supporting States in eliminating safe havens through the adoption of common offence elements;

(b) The development of international model provisions on investigative powers for electronic evidence, with a view to supporting States in ensuring the

[9] Further detail is provided in UNODC/CCPCJ/EG.4/2013/2.

necessary procedural tools for the investigation of crimes involving electronic evidence;

(c) The development of model provisions on jurisdiction, in order to provide for common effective bases for jurisdiction in criminal matters relating to cybercrime;

(d) The development of model provisions on international cooperation regarding electronic evidence, for inclusion in bilateral or multilateral instruments, including a revised Model Treaty on Mutual Assistance in Criminal Matters, in line with suggestions in the discussion guide for the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice;

(e) The development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters, with a view to providing an international mechanism for timely cooperation to preserve and obtain electronic evidence;

(f) The development of a comprehensive multilateral instrument on cybercrime, with a view to establishing an international approach in the areas of criminalization, procedural powers, jurisdiction and international cooperation;

(g) The strengthening of international, regional and national partnerships, including with the private sector and academic institutions, with a view to delivering enhanced technical assistance for the prevention and combating of cybercrime in developing countries.

V. Recommendations for promotion of activities relating to combating cybercrime, including technical assistance and capacity-building

53. The Commission may wish to request UNODC, based inter alia on the activities of UNODC as outlined in section II of the present report, to continue providing technical assistance to Member States in addressing cybercrime and urge Member States to provide extrabudgetary resources for that purpose in order to ensure long-term sustainable capacity-building in addressing cybercrime for developing countries.