23 January 2013

Original: English

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 25-28 February 2013

Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector

Executive summary

I. Introduction

1. In its resolution 65/230, the General Assembly requested the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.[1] Furthermore, in its resolution 67/189, the General Assembly noted with appreciation the work of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the Commission on Crime Prevention and Criminal Justice in due course.

2. The first session of the expert group 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.[2] The methodology for the study provided for the distribution of a questionnaire to Member States, intergovernmental organizations and representatives from the private sector and

[1] General Assembly resolution 65/230, Annex.
[2] E/CN.15/2011/19.

V.13-80339 (E)

academic institutions. Information gathering was conducted by the United Nations Office on Drugs and Crime, in accordance with the agreed methodology, from February 2012 to July 2012.[3] The present report contains an executive summary of the draft comprehensive study prepared by the Secretariat, based on information gathered, for consideration by the second session of the intergovernmental expert group on cybercrime.

II. Global connectivity and cybercrime

3. In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the Internet. Over 60 per cent of all Internet users are in developing countries, with 45 per cent of all Internet users below the age of 25 years. By the year 2017, it is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population. By the year 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 (IP) connectivity.

4. "Definitions" of cybercrime mostly depend 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 the core of cybercrime acts. 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 for any crime, rather than a broad, artificial "cybercrime" construct.

III. The global cybercrime picture

5. In many countries, the explosion in global connectivity has come at a time of economic and demographic transformations, with rising income disparities, tightened private sector spending and reduced financial liquidity. At the global level, law enforcement respondents to the study perceive 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 cybercrime acts 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,

[3] 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.

and “cashing out” of financial information. Cybercrime perpetrators no longer require complex skills or techniques. In the developing country context in particular, sub-cultures of young men engaged in computer-related financial fraud have emerged, many of whom begin involvement in cybercrime in late teenage years.

6. Globally, cybercrime acts show a broad distribution across financial-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.

7. Victimization surveys represent a more sound basis for comparison. These demonstrate that individual cybercrime victimization is significantly higher than for “conventional” crime forms. 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 across 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.

8. 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 IP addresses globally functioned as botnet command and control servers in 2011. Internet content also represented a significant concern for Governments. Material targeted for removal includes 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.

IV. Cybercrime legislation

9. 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 cybercrime acts. Countries increasingly recognize, however, the need for legislation in other areas. Compared to 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 perceive their criminal and procedural law

frameworks to be sufficient, although this masks large regional differences. While more than two-thirds of countries in Europe report sufficient legislation, the picture is reversed in Africa, the Americas, Asia and Oceania, where more than two-thirds of countries view laws as only partly sufficient, or not sufficient at all. Only one half of the countries, which reported that laws were insufficient, also indicated new or planned laws, thus highlighting an urgent need for legislative strengthening in these regions.

10. The last 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: (i) the Council of Europe or the European Union, (ii) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (iii) intergovernmental African organizations, (iv) the League of Arab States, and (v) 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.

11. Globally, 82 countries have signed and/or ratified a binding cybercrime instrument.[4] 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 the 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 is 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.

12. Overall, one-third of responding countries report that their legislation is highly, or very highly, harmonized with countries viewed as important for the purposes of international cooperation. This varies 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, in terms of cybercrime acts 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] One or more of: the Council of Europe Convention on Cybercrime, the League of Arab States Convention on Combating Information Technology Offences, the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information or the Shanghai Cooperation Organization Agreement in the Field of International Information Security.

V. Criminalization

13. Information on cybercrime criminal laws was gathered through the study questionnaire, as well as by primary source analysis of available legislation collected by the Secretariat.[5] The study questionnaire referred to 14 acts commonly included in notions of cybercrime.[6] 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 not mentioned in the questionnaire. These mostly concerned computer content, including criminalization of obscene material, online gambling, and online illicit markets, such as in drugs and persons. For the 14 acts, countries reported the use of cyber-specific offences for core cybercrime acts 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.

14. 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 regarding the criminalization of "mere" access or the requirement for 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 by virtue of whether the offence is restricted to non-public data transmissions or not, and concerning 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.

15. Several countries have adopted cyber-specific crimes for computer-related fraud, forgery and identity offences. Others extend general provisions on fraud or

---

[5] Primary source legislation was analyzed 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).

[6] 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.

theft, or rely on crimes 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 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, criminalization of possession and access shows greater variation. For computer-related copyright and trademark infringement, countries most usually reported the application of general criminal offences for acts committed wilfully and on a commercial scale.

16. 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 calls for respect for rights to freedom of expression. Responding countries report 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.

17. International human rights law acts both as 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 leeway to countries 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. Penal laws on defamation, disrespect for authority and insult, for example, that apply to online expressions 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.

VI. Law enforcement and investigations

18. Over 90 per cent of responding countries report that cybercrime acts most frequently come to the attention of law enforcement authorities through reports by individual or corporate victims. Responding countries estimate that the proportion of actual cybercrime victimization reported to the police ranges upwards from 1 per cent. One global private sector survey suggests that 80 per cent of individual victims of core 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 reputation 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 criminal scheme architects. Law enforcement authorities in developed countries are engaged in this area, including through undercover units targeting offenders on social networking sites, chat rooms, and instant messaging and P2P services. Challenges in the investigation of cybercrime arise from criminal innovations by offenders, difficulties in accessing electronic evidence, and from 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.

19. Law enforcement cybercrime investigations 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 ten cybercrime investigative measures, ranging from generic search and seizure to specialized powers, such as preservation of computer data.[7] Countries most often reported the existence of general (non-cyber-specific) powers across 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-situations, in many cases such an approach can also lead to legal uncertainties and challenges to the lawfulness of evidence gathering, and thus the admissibility of evidence. Overall, national approaches to cybercrime investigative powers show less core commonality than for criminalization of many cybercrime acts.

20. 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 report 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 a cybercrime act. 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.

21. 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

[7] 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.

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. 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 both 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 is a need to balance privacy and due process, with disclosure of evidence in a timely manner, in order to ensure that the private sector does not become a "choke-point" for investigations.

22. 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 on investigations. When investigations are transnational, divergences in levels of protection, however, give rise to unpredictability regarding foreign law enforcement access to data and potential jurisdictional gaps in privacy protection regimes.

23. Over 90 per cent of the countries that responded to the questionnaire have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence. In developing countries, however, these are not well resourced and suffer from a capacity shortage. Countries with lower levels of development have significantly fewer specialized police, with around 0.2 per 100,000 national Internet users. The rate is 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 receive training more than once a year. More than half of responding countries in Africa, and one-third of countries in the Americas report that law enforcement resources for investigating cybercrime were insufficient. Globally, it is likely that the picture is 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, Asia and Oceania reported requiring technical assistance. The most commonly cited area for technical assistance required was general cybercrime investigative techniques. Of those countries requiring assistance, 60 per cent indicated that this was needed by law enforcement agencies.

VII. Electronic evidence and the criminal justice response

24. 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 — often volatile and easily contaminated — information

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, across all regions, however, note insufficient numbers of forensic examiners, differences between capacity at federal and State level, lack of forensics tools and backlogs due to overwhelming quantities of data for analysis. One half of countries report that suspects make 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 lies 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 are typically lower than those of investigators. Globally, around 65 per cent of responding countries report some form of prosecutorial cybercrime specialization. Just 10 per cent of countries report specialized judicial services. The vast majority of cybercrime cases are handled by non-specialized judges, who, in 40 per cent of responding countries, do not receive any form of cybercrime-related training. Judicial training on cybercrime law, evidence collection, and basic and advanced computer knowledge represents a particular priority.

25. Over 60 per cent of responding countries do not make a legal distinction between electronic evidence and physical evidence. While approaches vary, many countries consider this good practice, as it ensures fair admissibility alongside all other types of evidence. A number of countries outside of Europe do not admit electronic evidence at all, making the prosecution of cybercrime, and any other crime evidenced by electronic information, unfeasible. While countries do 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 may have particular application to electronic evidence. Many countries highlighted challenges of attribution of acts to a particular individual and commented that this was often dependent upon circumstantial evidence.

26. The challenges facing both law enforcement investigators and prosecutors mean that "brought to justice" rates are low for cybercrime offenders. Suspects identified per police-recorded offence are comparable for child pornography offences to 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, show that the ratio of persons convicted to recorded offences, is significantly lower than for other "conventional" crimes.

VIII. International cooperation

27. Countries responding to the study questionnaire report that between 30 and 70 per cent of cybercrime acts involve 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 where an element or substantial effect of the offence is in another territory, or where 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 cybercrime acts, 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 to assert territorial jurisdiction. 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. Where 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 cybercrime acts and at least one State.

28. 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 preservation of computer data. Use of traditional forms of cooperation predominates for obtaining extra-territorial evidence in cybercrime cases, with over 70 per cent of countries reporting using formal mutual legal assistance requests for this 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 of 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 in Asia and Oceania, report channels for urgent requests. However, the impact of these on response times is unclear. Modes of informal cooperation are possible for around two-thirds of reporting countries, although few countries have 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 three per cent of the total number of cybercrime cases encountered by law enforcement for the group of reporting countries.

29. 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, due to cloud computing technologies which 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 where 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 Cybercrime Convention and the League of Arab States Convention on 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 presumed knowledge of the location of the data at the time of access or receipt.

30. The current international cooperation picture risks the emergence of country clusters that have the necessary powers and procedures to cooperate among themselves, but are restricted, for 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 common approach, including within current multilateral cybercrime instruments, means that requests for actions, such as 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.

IX. Cybercrime prevention

31. 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 report the existence of national law or policy on cybercrime prevention. Initiatives are under preparation in a further 20 per cent of countries. Countries highlight that good practices on cybercrime prevention include the promulgation of legislation, effective leadership, development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base, and cooperation across government, communities, the private sector and internationally. More than one half of countries report the existence of cybercrime strategies. In many cases, cybercrime strategies are closely integrated in cybersecurity strategies. Around 70 per cent of all reported national strategies included components on awareness-raising, international cooperation, and law enforcement capacity. For the purposes of coordination, law enforcement and prosecution agencies are most frequently reported as lead cybercrime institutions.

32. 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 also report that user and employee awareness must be integrated into a holistic approach to security. Foundational principles and good practice referred to include 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 do not take sufficient steps to protect systems or incorrectly perceive that they will not be a target.

33. 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 rights to seek, receive and impart information.

34. Public-private partnerships are central to cybercrime prevention. Over half of all countries report the existence of partnerships. These are created in equal numbers by informal agreement and by legal basis. Private sector entities are most often involved in partnerships, followed by academic institutions, and international and regional organizations. Partnerships are mostly used for facilitating the exchange of information on threats and trends, but also 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 (CERTs) and specialized research centres.

X. Key findings and options

35. 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 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 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 with a broader cybersecurity perspective.

36. Options to strengthen existing and to propose new national and international legal or other responses to cybercrime may include one or more of the following:

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

(i) The provisions could maintain the approach of existing instruments regarding offences against the confidentiality, integrity and accessibility of computer systems and data;

(ii) The provisions could also cover "conventional" offences perpetrated or facilitated by use of computer systems, only where existing criminalization approaches are perceived not to be sufficient;

(iii) The provisions could address areas not covered by existing instruments, such as criminalization of spam;

(iv) The provisions could be developed in line with the latest international human rights standards on criminalization, including in particular, treaty-based protections of the right to freedom of expression;

(v) Use of the provisions by States would minimize dual criminality challenges in international cooperation;

(b) The development of international model provisions on investigative powers for electronic evidence, with a view to supporting States in ensuring the necessary procedural tools for the investigation of crimes involving electronic evidence:

(i) The provisions could draw on the approach of existing instruments, including orders for expedited preservation of data, and orders for obtaining stored and real-time data;

(ii) The provisions could offer guidance on the extension of traditional powers such as search and seizure to electronic evidence;

(iii) The provisions could offer guidance on the application of appropriate safeguards for intrusive investigative techniques based on international human rights law, including treaty-based protections of the right to privacy;

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

(i) The provisions could include bases such as those derived from the objective territoriality principle and the substantial effects doctrine;

(ii) The provisions could include guidance for addressing issues of concurrent jurisdiction;

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

(i) The provisions would focus on practical cooperation mechanisms that could be inserted in existing instruments for the timely preservation and supply of electronic evidence in criminal matters;

(ii) The provisions could include obligations to establish electronic evidence fast response focal points and agreed timescales for responses;

(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:

(i) By way of complementarity to existing international cooperation treaties, such an instrument could focus primarily on a mechanism for requesting expedited preservation of data for a specified time period;

(ii) The instrument may also include specific cooperation provisions for further investigative measures, including supply of stored data and real-time collection of data;

(iii) The scope of application would need to be defined, but should not be limited to “cybercrime” or “computer-related” crime;

(iv) The instrument could require response within a specified time period and establish clear focal point to focal point communication channels, building upon rather than duplicating existing 24/7 initiatives;

(v) The instrument could include traditional international cooperation safeguards, as well as appropriate human rights exclusions;

(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:

(i) The instrument could include elements from all of the options above in a binding, multilateral form;

(ii) The instrument could draw on existing core commonalities across the current range of binding and non-binding international and regional instruments;

(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:

(i) Technical assistance could be delivered based on standards developed through model provisions as set out in the options above;

(ii) Technical assistance could be delivered through a focus on multi-stakeholder delivery, including representatives from the private sector and academia.