Distr.: General
21 February 2017

Original: English

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 10-13 April 2017

Deliberations at the first meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 17 to 21 January 2011

Summary by the Rapporteur

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 be convened prior to the twentieth session of the Commission, 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.

2. The first meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime was held in Vienna from 17 to 21 January 2011. (For the report on that meeting, see UNODC/CCPCJ/EG.4/2011/3.) The meeting had before it a draft provisional agenda (UNODC/CCPCJ/EG.4/2011/1) and draft topics for consideration in a comprehensive study on the impact of and response to cybercrime (UNODC/CCPCJ/EG.4/2011/2) prepared by the Secretariat. The Expert Group reviewed and adopted a short procedural report, a collection of substantive topics for consideration in the study, and a methodology and indicative timeline for the study, all of which were reported to the Commission on Crime Prevention and Criminal Justice at its twentieth session (see E/CN.15/2011/19, annexes I and II).

3. A summary of the substantive deliberations was commenced but could not be finalized, owing to a lack of resources. In its resolution 22/7 of 26 April 2013, the Commission invited the Expert Group to finalize and adopt the summary reports of its first and second meetings, held in Vienna from 17 to 21 January 2011 and 25 to 28 February 2013, respectively. At the meeting of the extended Bureau of the Expert Group, held on 1 December 2016, the Chair requested the Rapporteur to finalize the summary reports by the end of January 2017 and keep the Secretariat and the Chair informed about the progress of his work. Accordingly, the Rapporteur, Christopher

D. Ram (Canada), reviewed original notes, elements of the draft summary and recordings of the session in order to prepare and finalize the present summary.

4. The deliberations of the Expert Group were based on the agenda as adopted, the draft list of substantive topics, and a proposed study methodology, which was developed during the session. The present summary of deliberations complements decisions relating to the substantive scope or methodology of the study by reviewing both the substantive issues raised and the information provided by the experts at the first meeting. It incorporates views expressed by intergovernmental and other experts on a range of issues, including substantive issues of concern to Member States, the draft list of substantive topics and other topics proposed for inclusion in the study, and procedural and methodological issues relating to the conduct of the study itself. It reflects the agenda of the meeting, but as many issues were raised more than once, it follows to the extent possible a thematic approach.

II. Summary of deliberations

A. The problem of cybercrime (agenda item 2)

5. Experts discussed the prevalence of and roles played by information and communications technologies in their countries, and how those factors were linked to cybercrime. Most experts noted that cybercrime was increasing. They also noted that there were concrete and complex links between (a) the prevalence and use of technologies, both within Member States and regionally, and (b) the evolution of cybercrime. Cybercrime was seen as a universal, but not necessarily uniform, problem. Many speakers agreed that the problem was of global concern. A number of experts pointed out that complex patterns of offending and victimization, and the flow of data and proceeds of crime, in addition to other factors, produced effects that varied from one Member State to another. It was noted that the spread of technologies and the accompanying problem of cybercrime also raised questions related to national sovereignty, independence, governance, human rights and culture. Several experts mentioned the need to respect sovereign independence and cultural diversity, both when developing definitions of cybercrime and when considering domestic, transnational and global responses to it.

6. Several aspects of the problem of cybercrime recurred throughout the session:

(a) *Information technologies and computer networks*. Experts noted that information technologies and computer networks represented both an opportunity and a goal of internal and international development efforts and were also seen as a means of providing and maximizing the effectiveness of development aid and technical assistance. From that perspective, cybercrime was also seen as a factor that could jeopardize development opportunities. Ways and means to address it were therefore essential for all Member States. Experts also pointed out that, while cybercrime and related activities could have different effects in developed and developing countries, every Member State shared the incentives to promote development and protect it from cybercrime. More generally, they noted that, since computer networks allowed offenders in one State to exploit infrastructure and target victims in another, there were shared interests in preventing and combating cybercrime outside of the context of development;

(b) *The speed and extent of the evolution of both technologies and cybercrime*. Those factors posed a challenge for lawmakers, law enforcement and criminal justice systems, in particular in developing countries. Concerns were raised about the need to ensure that domestic laws, international instruments and technical assistance programmes were all kept up to date and that technical assistance was offered on an ongoing basis;

(c) *The transnational nature of computer networks and cybercrime*. Experts observed that the official entities responsible for responding to cybercrime and

protecting victims and infrastructure were subject to the constraints of sovereignty, comity and territorial jurisdiction, whereas the offenders themselves were not. That point was often raised, not only in the context of law enforcement and international cooperation issues, but also in relation to more general policy areas, the influence of human rights on the forms that criminalization of cyberconduct should take and the national or global regulation of technologies for reasons not necessarily related to crime;

(d) *The complexity of cybercrime, the speed with which it is committed, and the challenges those factors pose for criminal investigation and prosecution, both in terms of domestic investigative capacity and legal or other frameworks for international cooperation*. It was noted that the need to establish rapid or expedited investigative powers and reconcile them with rule-of-law safeguards posed a challenge for domestic legislators and investigators;

(e) *The challenges posed by the speed and transnational nature of cybercrime*. Those factors increasingly created problems in terms of expediency when dealing with cybercrime. In transnational cases, fast access to data was needed. However, the requisite use of formal mutual legal assistance channels and the rule-of-law safeguards of all the involved States substantially increased the time necessary to obtain data;

(f) *The increasing ubiquity of technologies and the issues generated in almost every aspect of life by those technologies*. From the smallest village to the highest level of global strategic and international relations, and in both public and private sector activities, the prevalence of technologies has an impact. Experts highlighted the work of their own Governments and efforts at the regional and subregional levels. They also welcomed and emphasized both the need for global responses and the engagement of the United Nations in developing and coordinating such responses.

7. Two general issues were raised with respect to responses to cybercrime:

(a) *The need for reliable and comprehensive global data about the nature and extent of the problem*. That issue was reflected in the mandate to conduct a study, and the agreed materials on substantive topics and methodology for the study, adopted by the first meeting of the Expert Group. Significant challenges in that regard included the very broad scope of the problem, the range of sources of information to be considered, the need to constantly update data and analysis to reflect its dynamic evolution;

(b) *The question of legal or other frameworks to regulate and coordinate international responses to cybercrime*. Differing views were expressed. Some experts argued that a new comprehensive and universal international legal instrument on cybercrime was needed to establish global consensus on effective responses and provide a clear international legal basis for them. Others maintained that the use of existing domestic and international legal regimes, and more ad hoc approaches to case-by-case cooperation and the delivery of technical assistance would be more effective.

8. Regarding the meaning of the term “cybercrime”, several experts highlighted that a single legal definition was not feasible. However, there was general agreement on the need for a descriptive or typological approach as a basis for the study and other research, and as a foundation for effective international cooperation. Most experts agreed that the typology developed in the 1990s and reflected in the Council of Europe Convention on Cybercrime was a good starting point, regardless of whether they supported the Convention itself as a viable legal instrument. That typology included consideration of new types of crime, only made possible by new technologies; the use of technologies to commit pre-existing or analogous offences, sometimes in new ways; and the fact that technologies were also often used by organized criminal groups, terrorist groups or others in order to facilitate offences, avoid detection, or conceal evidence or the proceeds of crime.

9. Several experts pointed out that the potential for using technologies to commit pre-existing crimes was very broad, which would prevent any sort of listing approach, both in the study or in other applications. However, it was also noted that a de facto list of specific offences had emerged over time in areas where there had been a consensus that new technology-related patterns of offending presented a serious or specific problem and could require international cooperation and coordinated international responses. The examples most commonly mentioned in that regard were the creation and dissemination of child pornography and new or expanded types of mass fraud.

10. Several policy or political challenges to possible consensus on the scope of cybercrime as a global problem were also highlighted. One such challenge was the growing reliance of Member States on technologies and networks as a form of critical infrastructure, and the resulting emergence of cybercrime and other threats as a national security or cybersecurity issue. It was noted that overlapping of cybercrime and cybersecurity issues was inevitable. Another challenge mentioned was the fact that, while there was no international consensus on the precise definition or scope of the term “terrorism”, it was clear that terrorist organizations could and did use technologies and networks. That fact posed challenges with respect to both the scope of the study and efforts to prevent and combat cybercrime and terrorism in general. Most experts agreed that problems related to cybersecurity and terrorism existed and required a response, but views differed on whether it would be appropriate or feasible to develop responses to those threats in the context of the Expert Group’s mandate and process.

11. Problems regarding the measurement and assessment of rates and trends in cybercrime were also considered. There was agreement on the need for accurate national and global information as an evidence base for future actions, both in the study and more generally, and a number of specific challenges were raised. Several experts pointed out that statistical information generally followed both reporting and prosecutions based on the legal definitions of offences. It was noted that this did not capture scenarios in which the use of technologies was a factual element, but not a legal requirement, or cases that were not successfully investigated or prosecuted and did not necessarily reflect the different approaches of Member States to criminalization. It was also noted that “dark”, or unreported, crime was a significant problem, as many cybercrime occurrences were never detected, and in some cases, victims did not report them. Service providers and other private sector entities were seen as an important source of information in that area because offences were sometimes reported to them instead of public authorities and the occurrence or prevalence of some offences could be assessed through technical means. The lack of statistical capacity and infrastructure in developing countries was also raised, both as a challenge and a possible focus of development aid and technical assistance efforts. It was also noted that technologies were spreading rapidly and transforming many governance, social and economic activities, thereby posing broader challenges to the assessment of the costs and general seriousness of the problem, and to statistical comparisons over time.

B. Responses to cybercrime by Member States, the international community and the private sector and options to strengthen existing and propose new national and international legal or other responses to cybercrime (agenda items 3 and 4)

12. In the area of existing domestic legal and other responses, many experts provided summaries of legislative measures in their countries, some spanning several decades, as cybercrime had expanded and evolved. Most experts indicated that their countries had recognized the seriousness of the problem and that action had been taken in the form of legislative and other responses. Different approaches were mentioned, but it was noted that those approaches generally reflected some combination of the amendment or modernization of existing criminalization

provisions under national law and investigative powers, and the establishment of entirely new provisions, where necessary. Most experts agreed that there was a need to protect the integrity of computer networks and their users from new and specific criminal threats such as malware, botnets, and the accessing of stored data or in-transit communications in ways that invaded individual privacy or national sovereignty. There was also agreement on the need for the establishment or modernization of offences in order to ensure that specific problems, such as fraud and child abuse, were addressed. Recurring issues with respect to legislative responses included whether the focus of amendments should be on modifying pre-existing offences and powers or taking entirely new approaches, and on the need to draft legislative provisions in a "technology-neutral" way so that they would not become obsolete or unenforceable as technologies evolved.

13. Many experts noted that some degree of harmonization or common approaches to criminalization was desirable in terms of providing a basis for international cooperation, but some also pointed out that there would not necessarily be consensus on every possible offence and highlighted the need to respect national sovereignty and cultural diversity. A range of different views was expressed on whether the best approach to harmonization and international cooperation was through the open-ended elaboration of a new international legal instrument, the use of the Council of Europe Convention on Cybercrime as a legal basis or "soft law" guidelines, the use of other existing instruments or guidelines, or a more ad hoc approach to case-by-case cooperation, information-sharing and technical assistance. Some experts noted, however, that there were limits on harmonization, as many States already had laws, and it would be necessary to share information so that each State could choose the best approach for itself.

14. Several experts pointed out that harmonization of criminal offences and investigative laws would also be linked to some degree to those human rights laws that affected access to and use of technologies and networks and the scope of offences and those linked to other areas, such as different approaches to the regulation of non-criminal uses of technologies, service providers and the setting of technical standards. For example, it was noted that some forms of online content were the subject of criminal offences in some jurisdictions while being covered by legal freedom of information or expression protections in others. Some experts mentioned discrepancies in general offences or specific cybercrime offences, such as differences in the ages of victims used as the basis for offences against children. Differences in the actual commission of offences and the advent of "distributed offending", in which complex offences were committed by groups of offenders in different places, were also raised as a challenge both to legislators and investigators.

15. A number of experts outlined their national legislative schemes regarding the investigation of cybercrime. In most cases, investigative powers included general powers governing techniques such as search and seizure, the interception of communications, and forensic and evidence rules and practices. More specialized provisions or variations developed specifically to address challenges in cybercrime investigations were also mentioned. Such challenges and measures included legal obligations on service providers to preserve data and assist investigators by retrieving and producing relevant data from complex systems and expedited investigative powers in response to the speed with which offences could be committed and digital evidence could be moved or erased if offenders became aware of an investigation. It was noted that a number of pre-existing investigative techniques had been adapted for use in locating, seizing and preserving digital evidence in devices and networks. Several experts also mentioned the challenge of keeping up with the constant evolution of technologies and offender techniques for avoiding detection or surveillance and the need for new investigative powers and techniques. In that context it was noted that some forms of malware could be used by law enforcement in much the same way as by offenders, but that such uses could raise significant rule-of-law, human rights or jurisdictional concerns, depending on the circumstances.

16. While the scope of the study and the mandate of the Expert Group were focused on domestic and international responses to cybercrime as a criminal law or criminal justice matter, a number of experts pointed out that non-criminal areas of law were critical to understanding domestic responses to the problem and building international consensus on how to respond to it. One such area raised was national and international human rights, which some experts indicated had direct effects on the scope of criminalization and on domestic and transnational investigative powers and practices. In that regard, it was highlighted that the willingness and legal ability of many States to cooperate would be contingent on having mutually satisfactory rule-of-law and human rights safeguards in place. The extent to which more general or proactive human rights measures such as data protection laws or standards were a factor was also raised. Experts also mentioned a range of non-criminal domestic laws that applied to various private sector or individual activities affecting both the infrastructure in which cybercrime takes place and the capacity or obligation of companies to cooperate in prevention and investigation. Common examples mentioned were laws or technical standards regarding privacy and data protection infrastructure, legal obligations to report offences or cooperate with law enforcement in various ways and legal obligations or voluntary practices with respect to matters such as encryption and technical security.

17. Regarding proposed or possible future domestic legal or other responses, there was general agreement that substantial advances had been made, starting in a few developed Member States in the 1980s and 1990s and then spreading more generally. Most of the experts described legislative and other efforts from the past few years, and many highlighted the development of national efforts to build capacity in order to keep abreast of new technological developments. The integration of efforts aimed at preventing and combating cybercrime into non-criminal areas such as governance, commercial development and national development strategies was highlighted. There was also general agreement on the need for development aid and technical assistance to ensure that cybercrime did not contribute to a "digital divide" among Member States or become a barrier to development. It was further generally agreed that efforts to suppress cybercrime in countries with strong legal and law enforcement capacity should not simply displace such a transnational and global problem to a country with weaker capacity. Several experts provided information about ongoing national and regional technical assistance efforts. Both national experts and private sector representatives also highlighted that that sort of crime prevention and capacity-building was an area where the private sector had both the incentive and ability to make a substantial contribution.

18. Regarding existing and proposed or possible international legal responses, a range of views was expressed and some significant differences with respect to possible approaches were raised. Different views were expressed regarding the criminalization of specific forms of conduct and investigative powers or methods, and many experts noted that, to the extent possible, harmonization of laws and common approaches to criminalization were desirable as a basis both for international cooperation and technical assistance. It was noted that cybercrime posed similar challenges everywhere and that there was a common interest in sharing legal expertise and identifying and addressing the gaps in criminalization or law enforcement that offenders could exploit.

19. A number of experts and several organizations made observations about the current and potential roles of international organizations. It was pointed out that several regional and subregional organizations were active in developing or maintaining legal frameworks or standards, including the Council of Europe Convention on Cybercrime, the Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information (2001), the Agreement on Cooperation in the Field of International Information Security, and relevant European Union standards and regulations. A range of research, development and technical assistance or capacity-

building activities was also mentioned. It was noted that there was a need for coordination of mandates and activities among entities and activities focused on cybercrime and related areas, including human rights, commercial and other non-criminal areas of public and private international law, and technology regulation. Many experts welcomed the initiatives of regional organizations, but several highlighted the fact that the global nature of computer networks and cybercrime made the involvement of the United Nations essential, and in particular, the Commission on Crime Prevention and Criminal Justice and the United Nations Office on Drugs and Crime (UNODC). Some experts welcomed the present study as the first major effort on that topic under the auspices of the Commission, while others called attention to previous consideration of cybercrime or computer crime by the Commission, the General Assembly and other bodies.[1] Several experts mentioned the United Nations Manual on the Prevention and Control of Computer-related Crime, which was developed in 1994, and suggested that it could be updated and re-issued.[2]

20. Regarding the possible elaboration of a new international legal instrument or convention on cybercrime, some experts expressed no views, while others exchanged a range of different views on the best approach. It was noted that the question had been the focus of political discussions and had led to an eventual compromise at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. The results of those discussions, contained in the Salvador Declaration, were the basis of the mandate of the Expert Group itself. In that context, some experts expressed concern that focusing on the nature of a possible legal framework for international actions against cybercrime could cause Member States or experts to overlook or underestimate the difficulty of addressing many of the specific challenges that such responses entailed, whether in the context of a legal instrument or not. It was also highlighted that the Salvador Declaration called for a study to examine options to strengthen existing measures and propose new ones. Those measures included legal and other measures responding to cybercrime, both national and international in scope, and it was noted that a balanced result to fairly examine all possible responses was needed.

21. With regard to the present study, some experts argued that, in procedural and methodological terms, it should include consideration both of the feasibility and desirability of such an instrument and of possible content or elements. Other experts argued that the purpose of the first part of the study was to collect and present factual evidence and that the consideration of legal responses would be a matter for consideration by the Expert Group, the Commission and other political bodies once the evidence had been assembled. There was general agreement that the eventual consideration of that issue was a matter for the Expert Group itself and that the study should examine options with regard to effective legal bases, including universal international bases and other responses for combating cybercrime (see E/CN.15/2011/19, annex I, para. 33 (b)). In that context, there was also

[1] See Economic and Social Council resolution 1999/23, entitled “Work of the United Nations Crime Prevention and Criminal Justice Programme”, E/CN.15/2001/4 and E/CN.15/2002/8; *Report of the International Narcotics Control Board for 2001* (United Nations publication, Sales No. E.02.XI.1), paras. 5-83; General Assembly resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001; *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: report prepared by the Secretariat* (United Nations publication, Sales No. E.91.IV.2), chap. I, sect. C, *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000: report prepared by the Secretariat* (United Nations publication, Sales No. E.00.IV.8), paras. 161-174 and *Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18-25 April 2005: report prepared by the Secretariat* (United Nations publication, Sales No. E.05.IV.7), paras. 323-340.

[2] *International Review of Criminal Policy*, Nos. 43 and 44 (United Nations publication, Sales No. E.94.IV.5). Experts mentioned that the update and reissuance of the Manual was previously recommended by the 2000-2001 study of cybercrime and the 2004-2007 study of economic fraud and identity-related crime. See E/CN.15/2001/4, para. 52 (a)(i) and E/CN.15/2007/8, para. 37 (g).

discussion of whether references to an "international legal instrument" implied instruments of a universal nature or also included instruments elaborated or open to ratification or accession only on a regional or non-universal basis. Some experts maintained that non-universal instruments agreed among two or more Member States such as the Council of Europe Convention on Cybercrime were still international legal instruments, whereas others argued that this term referred only to instruments of a universal nature.

22. In substantive terms, some experts maintained that ad hoc arrangements or legal instruments elaborated on a regional basis, in particular the Council of Europe Convention on Cybercrime, were not a sufficient response and that a legal instrument elaborated using an open-ended process and open to universal ratification or accession under the auspices of the United Nations was needed. They argued that the global nature of information and communications technologies and cybercrime made a universal legal instrument essential and pointed out that such processes and instruments were not a novel approach to addressing transnational forms of crime. Those experts also highlighted the importance of both the underlying consensus on responses to cybercrime as a basis to elaborate such an instrument and the importance of the United Nations as the only forum in which the issues involved could be effectively addressed. Several other specific concerns were also raised, including the need for open-ended negotiations and consensus-building, the unwillingness of some Member States to accede to the Council of Europe Convention on Cybercrime as an instrument they had no say in negotiating, and the inability of some Member States to accede to the Convention for policy reasons or owing to practical problems associated with specific provisions of the Convention itself. One such concern pertained to provisions of the Convention that allow some forms of direct cross-border investigation, and in particular, the possibility of directly accessing data based on the consent of private parties in possession or control of the data without necessarily notifying or obtaining the consent of the State in whose territory the data were physically located. Those experts also mentioned problems associated with the lack of a common legal or human rights framework and differences in policies, legal traditions or culture with respect to criminalization elements. Some of the experts who supported the open-ended elaboration of an international legal instrument also argued that the Council of Europe Convention on Cybercrime was already out of date or did not address other issues they thought should be considered or included.

23. Other experts maintained that the elaboration of a new international legal instrument on an open-ended basis was not feasible, given the urgency of the problem and the magnitude of some of the issues that would have to be resolved on a consensus basis. They noted that the issue had been raised in the Twelfth United Nations Congress on Crime Prevention and Criminal Justice and on previous occasions and argued that positions on a range of national sovereignty and domestic law issues were too divergent to allow for the elaboration of a useful and effective instrument within a reasonable time. They expressed the hope that the study would assist in clarifying the similarities and differences of approach in national laws and the extent to which consensus might be reached. In their view, the better approach was to focus on more immediate needs for technical assistance and the development of informal means of cooperation that would allow for expedited investigations. They maintained that, while sovereignty, jurisdiction and human rights could be factors, those challenges could not necessarily be addressed. They also felt that the primary problem facing law enforcement was the lack of national capacity and suitable informal channels, and that that should be the focus of future work. Those experts also argued that the complexity of cybercrime and the speed with which offences could be committed suggested a need for flexible case-by-case approaches, especially in respect of investigative techniques that were allowed in some jurisdictions but not in others. In that regard, they saw the building of reciprocal confidence among law enforcement authorities through the means available, such as "24/7" networks, as important. They also expressed concern that potential attempts to develop a new comprehensive international legal instrument on cybercrime would

take a considerable amount of time and success could not be guaranteed. On that basis, they argued that, to the extent that such an international legal framework was needed, the best possible option would be to use the Council of Europe Convention on Cybercrime, which had been developed within the context of the Council of Europe but was also open to accession by other States. A number of experts also mentioned that the Council of Europe Convention on Cybercrime was also valuable as a "soft law" option for the guidance of Member States as a basis for provisions on criminalization, investigative powers or electronic evidence, or other laws, even if those States were not willing or able to accede to and fully implement it.

24. In general, the discussion of a possible universal and comprehensive international legal instrument focused on the desirability or feasibility of its development, rather than on what that instrument might contain or the specific issues likely to be raised in negotiations. Several experts noted that, for them, the latter was an important element of the study, which would identify issues and challenges and suggest approaches to resolving them. One expert did raise more specific details, suggesting that the basic form of the United Nations Convention against Corruption could be followed regarding matters such as criminalization, prevention, technical assistance, international cooperation and the protection of national sovereignty. Another expert noted that, while global discussions of terrorism could be difficult, there would be at least some potential to consider extension of such an instrument to specific terrorist or related offences, and that some of the uses of technologies by terrorist groups would probably be covered by provisions directed at cybercrime in general.

25. The Organized Crime Convention was also mentioned in that context. Some experts considered the Convention a useful tool, given that most Member States had ratified or acceded to it. Furthermore, a significant amount of cybercrime appeared to be "transnational in nature" and involve an "organized criminal group", thus fulfilling the article 3 requirements for applying the Convention. Other experts noted that it did not extend to cybercrime scenarios, in which organized criminal groups were not involved, and that it did not fully address specialized forms of international cooperation that might be needed in cybercrime cases. Uncertainties over the seriousness of some forms of cybercrime and whether those would meet the "serious crime" threshold requirement for applying that Convention, as defined in its article 2 (b), were also mentioned. A similar range of views was expressed with respect to the application and usefulness of anti-terrorism instruments in scenarios where terrorists either attacked technologies or networks or used them for other purposes.

26. Several specific challenges were also raised in relation to existing or possible future legal frameworks for international cooperation, including the need for effective solutions to some of the general problems set out in paragraph 7 of the present report. Concerning international cooperation in general, a range of views was expressed with respect to how such cooperation could be afforded in a timely manner, whether under existing international and regional legal instruments, such as the Organized Crime Convention and the Council of Europe Convention on Cybercrime or on various bilateral or informal bases. A number of experts raised concerns with respect to the need for consensus on forensic standards for the collection, preservation, transfer, authentication and use of digital data as evidence in criminal or other legal proceedings. Some experts also pointed out that differences in national laws concerning the permissibility of techniques such as the interception of communications and the infiltration of criminal activities or impersonation or "entrapment" of offenders, could raise concerns in scenarios where online investigations were involved or affected other jurisdictions. Other experts also pointed out that differences could arise with respect to human rights requirements in national laws, using as an example differences in the privacy protections applied to the data used to direct and trace communications and the actual content of those communications.

27. Regarding transnational investigative procedures, a number of experts, particularly those with law enforcement backgrounds, argued that while conventional mutual legal assistance channels were necessary in transnational cases, they were no longer sufficient in cybercrime cases. They emphasized that the speed with which offenders could now commit cybercrime offences and then delete or conceal electronic evidence demanded much faster and more direct investigative powers and techniques. There was general agreement that the issue of speed posed a serious and expanding problem, but many experts also highlighted the need to respect national sovereignty, equality, independence and territorial jurisdiction. The latter group of experts argued that while mutual legal assistance mechanisms might be made more efficient, their basic function was to protect sovereignty and to prevent the circumvention of each State's basic rule-of-law requirements, including those implementing human rights and procedural safeguards. That was also one of the specific concerns raised with regard to the Council of Europe Convention on Cybercrime. One expert argued that the Convention went too far in allowing extraterritorial access to data, while another expressed the hope that the relevant provisions would be amended to go even further in that regard. Law enforcement experts generally felt that the gap between the short time frames of investigations and the much longer ones of international cooperation was the most serious challenge to the investigation and prosecution of transnational cybercrime cases. Several experts also pointed out that the problems were becoming steadily more serious as developments such as "cloud computing" increased the number of different jurisdictions likely to be involved in such cases and made physical locations increasingly less certain and harder to ascertain in the short times available. Experts also raised more general concerns about the need for practical formulas or understandings with respect to how responsibility for investigative and prosecutorial elements should be allocated among various jurisdictional claimants in scenarios involving a number of different States.

28. Several experts and representatives of the private sector highlighted the importance of prevention. Both technical means, such as the use of security applications to protect the integrity of systems and data, and social means, such as the education of system users and the inclusion of cybercrime elements in relevant school and university programmes, were mentioned. Experts noted that the very large scope and continuing nature of some cybercrime activities, including spamming and the operation of botnets, made it important to have the capacity to intervene while individual offences were being continually committed against new victims, often by devices running automatically. The ability to track down and remove malware from infected devices was seen as essential, both as crime prevention and as a reactive investigative measure. One related measure that was mentioned was the possibility of creating powers and the capacity to block or "take down" websites being used to commit offences or propagate illegal content or malware. There was also discussion on the criminal law, human rights, jurisdictional and technical issues that such a measure raised. Some experts pointed out that such a measure would entail both legal powers and the technical ability to trace and delete malware. Others noted that private sector operators of infrastructure could play an important role both in developing malware-resistant systems and in the removal of malware. It was also noted that public and private sector cross-border cooperation was important, since botnets were transnational in nature.

29. The important roles of the private sector and the need for effective public-private cooperation were raised in the context of the Salvador Declaration and the mandate for the study. A number of experts and private sector representatives raised issues related to public-private cooperation. It was pointed out that the range and evolution of private sector activities in different technical and regulatory environments made it difficult to define key terms such as "service provider" for legal purposes, but that this was not necessarily a problem for developing good cooperation practices. From a private sector perspective, it was pointed out that the challenge of meeting the legal requirements of different countries was a significant one for companies with international activities. It was also noted that, while

Governments tended to see the private sector as a single entity, it actually consisted of a vast array of entities with different functions and capabilities, which had important implications when various forms of assistance or cooperation were sought.

30. Several experts highlighted the need to identify and learn from successful efforts and the need to raise awareness in the law enforcement community of what the private sector could and could not do. Experts said that cooperation was possible and desirable in a fairly wide range of specific areas, including prevention, cooperation in investigations, collection of more general information about crime developments and trends, and training of investigators and forensic experts on new technologies as they were developed and marketed. One specific issue mentioned with respect to public-private cooperation in investigations was the extent to which legal safeguards applied when private companies engaged in investigative activities. Related issues included the application of judicial oversight and human rights safeguards, the protection of national sovereignty when transnational companies or activities were involved, and the admissibility of information obtained as evidence.

31. A number of experts highlighted the importance of technical assistance and information-sharing, both under the auspices of a comprehensive international legal instrument and on the basis of more immediate needs and means of delivery. It was noted that the same issue was identified as a separate and specific priority by the Salvador Declaration, and several experts emphasized that technical assistance was urgently needed and could not be deferred or delayed pending completion of the ongoing study. It was also noted that the nature of the problem required that such exchanges of information be reciprocal. Some experts pointed out that technical assistance related to cybercrime was also related to broader issues including development strategies and a range of specific efforts or projects. The Secretariat noted that UNODC had mandates to develop and deliver technical assistance and required only the necessary extrabudgetary resources to commence work. Experts representing other intergovernmental organizations present expressed the willingness to cooperate on technical assistance efforts.

32. The scope of the study and future work on cybercrime and their relationship to broader questions of cybersecurity and terrorism were raised at several points during the session. With regard to issues related to terrorism, consensus was eventually reached that the study should avoid broad-ranging or open investigations of terrorism. To the extent that it was raised, the focus should be on cybercrime itself in the context of terrorism (see E/CN.15/2011/19, para. 3). Several experts pointed out more generally that both cybersecurity and terrorism developments would pose challenges and create opportunities for possible synergies with respect to whatever future activities might result from the existing mandate of the Expert Group and the study itself. It was noted that, while Member States might regard some of the more serious threats as cybersecurity matters in policy terms, most of the actual activities involved would be within the scope of existing specific or general offences, or possible future work on cybercrime. Similar observations were made with respect to cyberterrorism. It was noted that the meaning of the term “cyberterrorism” was not very clear and that there was also no international consensus on the scope of the term “terrorism”. However, that fact did not necessarily preclude progress on reaching and implementing consensus on specific problems or activities. It was also pointed out that many online activities done in support of terrorist groups would be covered by more general offences.

C. A comprehensive study on cybercrime (agenda item 5)

33. The agreement of the Expert Group at its first session is documented in the annexes to its procedural report to the Commission on Crime Prevention and Criminal Justice (see UNODC/CCPCJ/EG.4/2011/3 and E/CN.15/2011/19). In considering options for the study, a number of issues and approaches were expressed. The Secretariat provided estimates of the costs of producing a study

document of 150 to 200 pages and of holding further sessions of the Expert Group. It also noted that, while the costs of the first session had been absorbed by the regular budget, further work by the Expert Group and within UNODC was contingent on the provision of extrabudgetary contributions. There was discussion of other options, including the use of smaller, less costly subgroups, but general agreement emerged that the study had to remain under the control of the Expert Group itself in order to ensure that oversight of the work and results remained both open-ended and intergovernmental. Most experts emphasized that the issues required consideration at the governmental level and that the process must remain open to all Member States. However, it was agreed that each regional group could nominate up to six governmental experts that the Secretariat could consult on specific issues on an ad hoc basis. Confidence was expressed in the neutrality of the Secretariat as the primary agency responsible for carrying out and reporting on the research, and it was emphasized that the eventual results would be subject to review by the open-ended intergovernmental Expert Group before transmission to the Crime Commission on Crime Prevention and Criminal Justice.

D. Conclusions and recommendations, adoption of the report and closing of the meeting (agenda items 6 to 8)

34. As noted above, the Expert Group adopted a short procedural report by the Secretariat, in addition to the collection of substantive topics to be covered by the study and methodology for the study as considered and amended during the meeting. Apart from that, no specific conclusions or recommendations were proposed or considered.[3] It was agreed that reports on the results of meetings of the Bureau of the Expert Group would be produced and circulated by means of the regional groups. The Rapporteur indicated that, in addition to the adopted substantive and methodological texts, a report summarizing the deliberations of the Expert Group would be prepared and circulated for approval as soon as it could be processed and distributed in all six official languages.[4]

[3] Further information on agenda items 6 to 8 is contained in the report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime held in Vienna from 17 to 21 January 2011 (E/CN.15/2011/19).

[4] As noted in paragraph 2 above, this was not done following the first (2011) and second (2013) sessions due to a lack of resources.