Distr.: General
24 February 2017

Original: English

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

Deliberations at the second meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 25 to 28 February 2013

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, annexed to that resolution, 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.

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 deliberations of that meeting, see UNODC/CCPCJ/EG.4/2017/2). At that meeting, the Expert Group reviewed and adopted a short procedural report (UNODC/CCPCJ/EG.4/2011/3), a collection of substantive topics for consideration in the study, and a methodology and indicative timeline for the study, which were presented to the Commission at its twentieth session. A summary of the substantive deliberations was prepared but could not be finalized owing to a lack of resources. The second meeting of the Expert Group was held in Vienna from 25 to 28 February 2013; because of resource constraints, only a short procedural report was transmitted to the Commission.

3. In its resolution 22/7, the Commission called for the finalization and adoption of the summary reports of the first and second meetings of the Expert Group. 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 to 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 in order to prepare and finalize the present summary.

4. At the second meeting, the Expert Group had before it a draft provisional agenda (UNODC/CCPCJ/EG.4/2013/1/Rev.1); the draft comprehensive study on cybercrime; and an executive summary of the comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector (UNODC/CCPCJ/EG.4/2013/2).

5. The Expert Group considered the draft comprehensive study and the methodology and work done to produce it. There was general agreement that the draft comprehensive study represented a major accomplishment and a significant contribution to the understanding of cybercrime, but a number of concerns were expressed about specific elements of the text. Given the length of the text, it was not possible to review it in detail in the limited time available during the meeting, and many experts indicated that they had not had sufficient time prior to the meeting to review it. The Expert Group was not able to reach a consensus on the text. Due to resource constraints, only a short procedural report was transmitted to the Commission, with a recommendation that the Commission consider the study further at its twenty-second session.

6. During the second meeting of the Expert Group, in response to several requests, a representative of the Secretariat gave a presentation, highlighting the work of the UNODC Global Programme on Cybercrime. He explained that the Global Programme had been under development for some time; however, it had only recently been approved and materials detailing it were being disseminated to Member States. The representative thanked the Governments of Norway and the United States of America for their initial support and outlined the proposed scope of work, which focused primarily on the development and delivery of technical assistance, both on cybercrime specifically and in coordination with other work of the United Nations Office on Drugs and Crime (UNODC) and other international and regional organizations. He also noted that the Global Programme could function as a repository of information generated by the study, together with other sources of information and legislation provided by Member States. During the meeting, the Secretariat confirmed that the work of the Global Programme would, as with other work of the Secretariat, be governed by the standing human rights considerations and requirements applicable to the United Nations as a whole. It was noted that, while the results of the draft comprehensive study should be used to support the work of the new Global Programme, oversight of the programme and its work was not within the mandates of the Expert Group.

II. Summary of deliberations

A. Presentation of information gathered and work done to conduct a draft comprehensive study of the problem of cybercrime in accordance with General Assembly resolution 65/230 (agenda item 2)

7. Experts raised a number of specific concerns about the progress and methodology of the Expert Group. Some speakers expressed concern that the work had fallen behind the schedule of the indicative timeline adopted by the Expert Group at its first meeting and expressed the hope that it would now be completed quickly so that the Commission could consider the problem. The Secretariat provided an overview of the steps taken thus far and noted that the length of time needed was not excessive in view of the size of the task and limited resources available. The work

involved the following: (a) the development and translation of survey materials; (b) the collection of information from 69 Member States and 67 private sector, academic and intergovernmental sources; and (c) the analysis of data and the drafting and dissemination of the text (287 pages).

8. Other experts expressed concerns about the lack of time available to review the draft comprehensive study, particularly given its size and complexity. Those concerns included both the fact that the draft text was released only a few days prior to the meeting and the lack of time during the meeting itself to review the text in detail. A number of experts informed the Expert Group that any comments were only of a preliminary nature and that they reserved the right to comment on specific elements of the text at a later time, on the basis that it was still under review in their countries at the time the meeting was being held. It was also noted that, for lack of resources, the text had not been translated into all official languages of the United Nations, which made it more difficult for many experts to comment on its content and participate fully in the work of the Expert Group. In that context, it was also noted that the document could not be treated as an official document of the United Nations.

9. With regard to reports on the work of the Expert Group, the Chair informed the Expert Group that the General Assembly required summary reports to be short and action-oriented, and to not contain any discussion or summaries of deliberations. Some experts expressed concerns about strictly procedural reports; in their view, the authority cited applied to texts developed within the Secretariat and not to deliberations of intergovernmental bodies. It was also stated that documenting the work of substantive expert bodies was not adequately served by such limited reports. One expert indicated that although some compromise was possible given the resource constraints, a purely procedural report was not acceptable to her Government. The Rapporteur noted that it had not been possible to produce and disseminate a summary of the substantive deliberations of the first meeting and that the Bureau had been informed that available resources would only permit a short procedural report on the second meeting. Several experts expressed the view that some substantive documentation of the deliberations would be essential for the Expert Group to complete its work. Some highlighted the importance of such documentation, both to inform future proceedings of the Expert Group and to inform others about its work. Other experts expressed the view that, given the intergovernmental nature of the Expert Group, the views and range of opinions expressed during the meetings were an element of the mandated study itself and needed to be documented or reported for that reason. The Secretariat confirmed that resources allocated from the regular budget of the United Nations were only sufficient for the translation and processing of a nine-page procedural report and that extrabudgetary resources would be required for anything longer than that. Further discussion of the matter was deferred to the Commission.[1]

10. With regard to the text of the draft comprehensive study, there was general agreement that the text produced by the Secretariat was a major and comprehensive effort, especially given the short time frame, the limited resources and the unprecedented nature of the effort required. It was seen as a valuable addition to the global understanding of the problem of cybercrime, not just for the immediate work and mandates of the Expert Group and the Commission, but also for long-term and

[1] The matter was taken up by the Commission on Crime Prevention and Criminal Justice at its twenty-second session. In paragraph 6 of its resolution 22/7, the Commission invited the open-ended intergovernmental expert group to finalize and adopt summary reports of its first and second meetings. However, the finalizing of the reports remained subject to the availability of extrabudgetary resources, which were not available until late 2016, at which time the present summary was prepared.

ongoing efforts to find effective responses to a major and constantly evolving global crime problem. Most experts also agreed that the responses reflected a reasonable balance of the different regions and levels of development and the different national, intergovernmental, academic and private-sector perspectives. However, a number of experts indicated that based on their preliminary view, the findings and results in the text and executive summary did not always appear to be based on or supported by the data and that, in some cases, alternative interpretations of the data needed to be considered and reflected in the text. Several experts highlighted the importance of having a balanced text, in particular to dispel misunderstandings about global cybercrime patterns and to better inform the planning and delivery of technical assistance. One expert highlighted that the majority of offenders and victims were in developed countries, and another observed that the uneven development of computer and communications networks meant that forms of crime that had existed for some time in one place might present new challenges somewhere else.

11. Several experts suggested that the raw data and information collected should be made available so that the Expert Group could review it, assess the detail or quality of the responses and comment on the analysis and findings. Such data and information could also be used by outside experts and organizations. The Secretariat indicated that such disclosure was not United Nations practice. Most of the data had been gathered on the basis of assurances of confidentiality, and further disclosure would require the consent of many of the sources. Several experts suggested that the data should be retained in the context of more general proposals, for example, that UNODC should assume a role as a repository of legislation and other information about cybercrime.

12. A range of views and concerns was expressed with respect to further work on the draft comprehensive study and its transmission to the Commission. While there was agreement that the length of the text was appropriate, it was noted that it nevertheless posed a problem with respect to reviewing, adopting and transmitting a final version to the Commission. A number of experts also pointed out that the Expert Group itself represented a valuable collection of substantive expertise on cybercrime and that the limited time it had to meet should, to the extent possible, be focused on the substantive issues raised in the draft text, while political and procedural questions should be left to the Commission.

13. There was no consensus on specific recommendations regarding the content of and findings and options in the draft comprehensive study or on how the work should proceed, apart from recommending consideration by the Commission of the draft comprehensive study, but there was general agreement on a number of substantive and procedural issues. Regarding the procedures and ongoing work of the Expert Group, the experts agreed that the mandate had to be respected and that any conclusions and recommendations had to emanate from the Expert Group itself, as an open-ended intergovernmental body comprised of experts, and on the basis of a consensus. Experts had different views on the context in which further work should be done, but there was general agreement that the magnitude and constant evolution of the problem of cybercrime made the ongoing intergovernmental and multi-stakeholder process to consider specific problems and responses necessary. Concerning the scope of the mandate and future work, there was also general agreement that the concept of cybercrime could be described but not defined, which meant that both links and synergies with respect to work in other areas, including cybersecurity, electronic commerce and telecommunications standard-setting and the global fight against terrorism and transnational organized crime, were inevitable.

14. There was also agreement on a number of substantive issues, bearing in mind that the limited time available did not permit discussion of many of the specific issues and challenges highlighted in the draft comprehensive study. There was general

agreement that cybercrime was increasing, both in terms of the volume of offences and the scope of illicit activities; that interconnectivity influenced crime patterns and increased transnational offending in particular; and that issues related to information technology were becoming a significant element in a broad range of non-cybercrime offences. A range of views was expressed concerning the scope and legal basis for technical assistance, but there was general agreement that such assistance was urgently needed and should be provided upon request and based on an assessment of the specific needs of each requesting Member State.

15. There was also general agreement that human rights issues would be important in analysing the scope of criminal offences and law enforcement powers and that a balance needed to be struck between effective investigative powers and human rights-based limits on those powers. It was noted that different human rights approaches and standards could also be significant factors in international cooperation, especially where investigative cooperation and the admissibility of extraterritorial evidence were concerned. Several experts pointed out that freedom of expression and privacy and other human rights should be the same in online and offline environments. Some experts pointed out that most countries had some limits on expression in cases where content was harmful, offensive or immoral and that the precise demarcation between what was protected and what was prohibited varied from one State to another.

16. Experts agreed that a multi-stakeholder approach that included academic, private sector and other interests would be needed to develop effective measures to prevent and respond to cybercrime. Most experts also agreed that there would be a need to establish and enhance public-private partnerships, with the nature of the partnership depending on the nature of the cooperation. Generally, the experts discussing the need for cooperation in investigative and other enforcement matters and for awareness-raising tended to focus on cooperation between public authorities and service providers, while those discussing cooperation related to capacity-building focused mostly on cooperation with manufacturers. It was noted that some form of structure or mechanism to support and regulate those partnerships and cooperative efforts might be needed and that, in some scenarios, private sector entities could and did cooperate with one another and with Member States on a transnational basis. One expert, representing the private sector, presented a number of examples of transnational cooperation in which his company had been involved.

17. A range of views was expressed with respect to criminalization and the formulation or adaptation of specific offences. It was noted that time did not permit a detailed discussion of specific offences and that the use of computers and networks to commit conventional crimes in new ways had created a very large, if not open-ended, range of possibilities. Experts highlighted that there was general consensus within the Expert Group and elsewhere on the need to establish and maintain appropriate criminal offences and fairly broad agreement on a core set of harmful activities, although the formulation of offences might vary. Several experts also noted, however, that there were activities that could be criminalized in one country and permitted or even protected in others, and examples of those activities were discussed.

18. With regard to investigative, prosecutorial and judicial capacity, there was general agreement that expert capacity was needed everywhere, which made it an important element of capacity-building efforts, and that frequent reviews were required to ensure that expertise kept pace with the evolution of technologies and crime. A related point of agreement was the need for awareness-raising among officials in general, combined with the referral of cases to specialized experts. A number of experts reported successful efforts to create specialized expert investigative units and prosecutors who could be assigned to specific domestic cases and foreign cooperation requests as needed. However, it was noted that, at the very least, basic

levels of expertise were rapidly becoming a requirement for almost all law enforcement personnel because the majority of non-cybercrime offences were increasingly involving investigative information and evidence that required some understanding of computer searches and digital forensics.

19. Experts agreed that the conflict between investigative needs for fast access to data and delays resulting from efforts to meet rule-of-law and human rights "due process" requirements remained a serious concern. It was noted that when such problems arose in connection with domestic investigations, they could be addressed with expedited powers and safeguards under national law. However, the same problems became much more serious in transnational cases. Formal mutual legal assistance or other official channels were needed in transnational cases to ensure that the rule-of-law and procedural safeguards were not circumvented, but the added stages were time-consuming and investigations became even more difficult if requests to two or more other countries were needed. Regarding any sort of direct access, most experts expressed the view that while computer networks made direct access to extraterritorial data possible, national sovereignty and rule-of-law requirements were paramount. They emphasized that continuing dialogue would be needed within and among Member States to find practical measures to at least reduce the problem.

B. Review of draft content and findings of the study in respect of the problem of cybercrime and responses to it 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)

20. A representative of the Secretariat provided an overview of the mandate given by the General Assembly to the Expert Group and the methodology for the study adopted by the Expert Group at its first meeting (see E/CN.15/2011/19, annexes I and II), outlined the steps taken by UNODC to collect and analyse the data and explained how those steps were reflected in the documents before the Expert Group. He indicated that information had been compiled and analysed in sections based on the requests made at the first meeting of the Expert Group and the resulting structure of the questionnaires. He also indicated that key findings and options had been compiled and set out in the executive summary, but that no proposed conclusions or recommendations had been included. He noted that efforts had been made to ensure that the text was as comprehensive as possible but it was not exhaustive and that, insofar as the quality of the data and length of time needed to collect and analyse the data were concerned, the experience of preparing the study had generally been consistent with other research efforts. He also noted that the number of responses and the level of completion were equal to, or better than, those of other similar efforts and the results reflected more detail than the results of most of the other efforts. He expressed confidence that the data provided were valid and reliable. The responses of Member States suggested consistency in how the questions had been interpreted and understood, and there was also general consistency among the responses of Member States, academic and private sector experts and the other sources reviewed regarding how the problem of cybercrime was understood, bearing in mind that a range of views had been expressed regarding possible responses to it. Regarding the options included in the executive summary of the draft comprehensive study, the representative of the Secretariat noted that those options had been compiled using responses from Member States to a specific question on what options they thought should be considered to strengthen existing or propose new international legal or other responses to cybercrime, based on the mandate of the Expert Group and the approval of the content of the draft questionnaire by the Member States.

21. Some experts expressed the view that the draft comprehensive study reflected a comprehensive range of options for responding to cybercrime and was based on an objective and impartial review of the data. They noted that the options put forward by the Secretariat reflected what had been said by Member States and were not necessarily alternatives, nor were they mutually exclusive. They noted the general agreement of the group that responses needed to be developed on an urgent basis and argued that any further choice or elaboration of options was a matter for Member States to take up at the next session of the Commission. On that basis, they argued that the entire text should be transmitted to the Commission for its consideration as soon as possible and that the Expert Group should not be selective or narrow the range of options transmitted or recommended to the Commission. In that context, they noted that it was not necessarily essential that the Expert Group complete its review of the study before referring it to the Commission in its existing form for the advice of the Commission or to seek further direction as to how to fulfil its mandate.

22. Other experts expressed concern about the lack of time available to review such a large text, both before and during the meeting, and some of those experts reserved the right to comment further when time permitted. They noted that standard United Nations practice required a detailed review of and consensus on each paragraph before the draft text could be adopted by the Expert Group and that such a review was not possible given the very limited time and resources available. The experts also noted that consensus appeared to be emerging in support of some options but not others, and they maintained that it was the mandate and function of the Expert Group itself to review the evidence, analysis and options prepared by the Secretariat. In their view, it was the Expert Group that should decide which, if any, conclusions and recommendations should be transmitted to the Commission and that such decisions should be based on an issue-by-issue consideration and consensus within the Expert Group. Those experts maintained that the development of concrete options prior to the review of the data by the Expert Group was premature. They also expressed the view that some of the findings and options were not necessarily supported by the data and that further, more detailed discussion of how they had been reached was needed. A number of those experts suggested that there was a disconnect between the data in the draft comprehensive study and the findings and options, and some of those experts felt that different interpretations of the evidence ought to be considered. Some of those experts also suggested that, while the mandate of the Expert Group focused on options to strengthen existing measures and propose new ones, the present scenario of continuing to expand the use of existing legal instruments and informal cooperation mechanisms should also be considered as an important option.

23. With regard to the current international legal framework, the representative of the Secretariat explained that the draft comprehensive study described the situation as one of fragmentation, with six or seven international legal instruments developed on a regional basis, each with a different scope and requirements, especially insofar as procedural powers were concerned. In reviewing elements of the draft comprehensive study, he suggested that efforts thus far had produced several clusters of instruments based on regional and subregional relationships, which led to greater or lesser access to binding cybercrime instruments depending on where a State was located. The representative noted that a majority of States tended to use bilateral instruments or arrangements where possible. A number of experts pointed out that those differences arose from differences in legal systems and diversity of approaches to cybercrime itself and not from the instruments, several of which were available to all Member States. Some experts felt that the term “fragmentation” suggested investigative barriers and that the term “differentiation” might be more appropriate, since it suggested the need to find ways to cooperate with and understand different legal systems. One expert pointed out that legal diversity reflected deeper differences and

that trying to reconcile or overcome those differences in negotiations might drive Member States to a very narrow consensus.

24. The Expert Group discussed chapter 3.2 of the draft comprehensive study, which assessed the degree of diversity in cybercrime legislation, finding that there was insufficient harmonization of offences, investigative powers and electronic evidence laws to support effective international cooperation. A number of experts raised concerns about those findings. Most experts agreed that, in general terms, similar approaches to criminalization and investigative powers could be useful both in the sense that legal instruments or model laws could be helpful to legislators developing or modernizing laws and in bridging gaps when dealing with transnational cases. However, it was noted that Member States were sovereign and often took different approaches to criminal justice matters. In that context, the view was also expressed that the essence of international cooperation was not to make laws identical but to develop effective channels of communication or bridges between different legal systems. Several experts observed that even States that had fully implemented the Council of Europe Convention on Cybercrime had retained significant substantive and procedural differences. Several experts pointed out that, while lack of coverage by basic criminal offences had in the past led to problems with dual criminality, most Member States had eventually established the necessary offences, and that the impediments to cooperation tended to be more in the realm of practical problems associated with lack of capacity. Several experts pointed out that cybercrime was no longer seen in their countries exclusively as a crime prevention and criminal justice issue. They also noted that cybercrime had important implications in other areas, ranging from economic, trade or technological development interests to national security or cybersecurity aspects.

25. With regard to international cooperation, most experts agreed that increased and faster cooperation would be needed to address the problem of cybercrime, especially as that problem continued to expand and reliance on technologies for legitimate purposes made the potential threat of cybercrime more serious. Beyond that, different views were expressed regarding the best strategic approach and priorities for addressing the problems related to cybercrime. Some experts considered the urgent elaboration of a universal legal instrument as the preferred priority. Others noted that, while the draft comprehensive study had suggested that the lack of universal instruments led to greater use of bilateral instruments, other factors, such as the size of the Member State concerned, needed to be considered. Those experts noted that smaller States tended to rely on multilateral instruments such as the United Nations Convention against Transnational Organized Crime, whereas larger ones tended to negotiate more detailed and advantageous bilateral agreements based on capacity and demand and to use those agreements instead. Other experts felt that the weakest link in international cooperation was not the lack of a legal framework but the lack of capacity. Those experts urged Member States to focus as a priority on technical assistance to address that problem. A number of experts mentioned the use of joint investigation arrangements, the use of “24/7” networks and other channels for direct communication, and it was suggested that the effectiveness of such channels be studied.

26. More generally, arguments raised for and against the elaboration of a universal legal instrument were similar to those raised during the first meeting of the Expert Group. Supporters of a universal instrument saw it as necessary for more structured, formal and mandatory coordination and cooperation, whereas others argued that the nature of cybercrime made faster and more informal channels of cooperation more important and that confidence-building and personal relationships were needed.

27. Experts who favoured a new universal legal instrument generally argued that the fundamentals of sovereign independence and different approaches to criminalization, procedural powers and other matters should be addressed formally, both in a formal negotiation process and in a consensus-based substantive text. They argued that a legal framework and capacity-building were interdependent in the sense that legal authority was not useful without capacity, but that capacity also required a legal basis if it was to be used in support of international cooperation. Some of those experts also indicated support for some elements of existing instruments, including the criminalization typology of the Council of Europe Convention on Cybercrime. They stated that those elements could form at least a starting point for the elaboration of a new instrument but that an open-ended process was needed to identify and respond to the full range of national differences. In more practical terms, experts also noted that while the Council of Europe Convention on Cybercrime was open to accession by non-member States of the Council of Europe, such accession required an invitation based on the unanimous consent of the States parties to the Convention, which, they noted, was a difficult requirement for many States to meet. Some experts also highlighted that their Governments could not accede to a Council of Europe instrument, either because they had not been able to participate in its development or for other concrete legal, policy-related or political reasons. In that context, those experts argued that the Member States that had joined or supported the Council of Europe Convention on Cybercrime should not block attempts by other Member States to attempt to elaborate a universal legal instrument in an open-ended process.

28. The experts who favoured alternatives to a new instrument raised additional concerns about the infeasibility of such an instrument in substantive or procedural terms. Some of those experts highlighted the differences that would have to be overcome in areas such as the scope of criminalization and human rights constraints on offences and investigative powers. There was also the difficult question of reconciling the need to respect principles of sovereign equality and territorial integrity with the need for either fast or direct access to extraterritorial data. Those experts also drew attention to the length of time that might be needed to elaborate an entirely new instrument, and they expressed concerns that a universal legal instrument would result in the lowering of existing standards or a weakening of existing powers or protections. Concerns were also expressed that an impasse or prolonged negotiation process could create a negative atmosphere and adversely affect existing informal cooperation. Those experts argued that the lack of consensus in recent United Nations congresses on crime prevention and criminal justice and the intervening sessions of the Commission underscored the above-mentioned difficulties and challenges. Those experts also argued that the Expert Group was the most appropriate forum to discuss the merits of the possible substantive and procedural responses to cybercrime and that the failure of the Expert Group to reach consensus at the second meeting was evidence of the difficulties that would arise if an open-ended treaty-making process were commenced.

29. A similar range of views was expressed with regard to the options of developing “soft law” texts such as model laws. It was noted that a number of model laws already existed and that some of the existing regional instruments were also being used as models or guidelines by Member States that were unwilling, unable or ineligible to accede to them. Experts who supported a universal legal instrument argued that efforts to produce model laws would be useful as an interim measure and a process in which issues could be explored and consensus could be gradually developed for an eventual universal convention on cybercrime. However, those experts who did not see such a convention as being feasible argued that nothing would be added to the existing understanding of the issues and options and that efforts and resources should instead be focused on the more immediate need for capacity-building.

30. There was general agreement among experts that international cooperation was essential and that work to improve it was needed. Experts who favoured a universal legal instrument as the basis for formal cooperation also favoured more formal and multilateral approaches, whereas those who thought such a legal instrument was not feasible tended also to emphasize more informal and personal relationships between agencies and individual specialists and the development of more specific bilateral or regional instruments or arrangements, where possible. In discussions, experts noted that, on the one hand, informal bilateral cooperation could not be a substitute for formal cooperation and rule-of-law protections; on the other hand, informal bilateral cooperation had the potential to bridge gaps in scenarios where formal multilateral frameworks would be difficult to develop among different legal systems.

31. Some experts argued that the Council of Europe Convention on Cybercrime was out of date as it lacked specific references to problems that had arisen since 2001, including phishing, botnets and crime in virtual worlds. Other experts argued that the Convention used technology-neutral language that applied to such problems. The representative of the Council of Europe explained the ongoing use of the interpretive guidance notes and the procedures for elaborating further protocols to amend the Convention where those procedures did not suffice. He also clarified that participation in any processes to develop amending protocols was open to all States parties to the parent Convention. Experts noted in that context that technology neutrality was an important consideration in developing any new legal provisions, whether at the national or international levels. It was also noted that concerns about the need to keep laws up to date with technological development applied equally to domestic laws, existing international legal instruments and any new universal or other legal instruments that might be developed in the future.

32. Experts noted that time did not permit a comprehensive review or detailed discussion of issues relating to domestic investigative powers and techniques, but some experts made general comments. There was general agreement that investigative expertise and capacity within each State were critical to both domestic law enforcement and international cooperation and that they should be a primary focus of technical assistance, where needed. It was also agreed that domestic expertise and technical assistance needed to be constantly reviewed and updated in order to keep pace with the evolution in technologies and their misuse by offenders. Several governmental and private sector experts also highlighted the potential role that companies could play in that area. Discussion of non-investigative enforcement options was limited, but a number of experts mentioned the need for the authority and capacity to take down websites or devices used for illegal purposes; in that context, numerous references were made to the dissemination of botnets and other malware. Several experts who had such authority and capacity reported on how they were used. Experts noted that the draft comprehensive study had not gone into much detail on non-investigative enforcement options. It was suggested that a further and more detailed exploration of it would be useful, both in the context of domestic enforcement and transnational enforcement requests.

33. Issues relating to data protection, including individual privacy and other rights, were mentioned by a number of experts in different contexts. Broader questions pertaining to the protection of economic interests and public confidence in data-storage and information infrastructures were also highlighted. In addition, experts mentioned that it was the sovereign prerogative of each Member State to control access to data within its territory and to establish and enforce powers and safeguards regarding lawful access to that data by domestic or foreign investigators. It was noted that while States usually sought to achieve a balance between data-protection and investigative interests, the actual balance and procedures involved could differ from

one State to another, and some experts regarded that as an important consideration for those involved in formal or informal cross-border investigative cooperation.

34. As in the first meeting of the Expert Group, several experts mentioned the continuing problem posed by the time taken to apply legal safeguards, on the one hand, and the need for fast, "real-time" investigations on the other, in particular in transnational cases. A representative of the Secretariat provided an overview of that and other cooperation issues, which were discussed in chapter 7 of the draft comprehensive study. It was noted in the study that, outside of Europe, many States had reported concerns with both cooperation in general and the speed of responses, which could be measured in months rather than days. He called attention to the discussion in the text of extensions of territorial jurisdiction based on concepts of objective territoriality and the effects doctrine. He also called attention to the suggestion that there was a need to reconceptualize the locations of data. Requests or orders to produce data were sometimes directed at the jurisdictions of companies that controlled the data or the data storage infrastructure rather than being directed at the jurisdictions of the States in whose territory they were stored. The representative of the Secretariat also noted that Member States had reported using direct means to obtain extraterritorial data that would not necessarily be permitted in their own territories and legal systems.

35. A number of experts expressed their concerns and the views of their Governments about issues relating to sovereignty, territoriality and jurisdiction. Most of those experts noted that while there was a need for more expedited forms of cooperation, basic attributes of national sovereignty and the rule of law within the territory of each Member State were paramount. Experts also said that cross-border investigative measures, especially those of an intrusive nature, had to respect international law and national laws and must not be undertaken without the awareness and consent of the territorial State. Experts said the issue had to do with sovereignty and the rule of law, because any legal rules and mechanisms a State might choose to enact and apply would be circumvented if extraterritorial investigative measures that would otherwise involve them were taken directly and without notification or consent.

36. Experts who expressed views on those issues generally said that complete solutions might not be possible, but that approaches to the problem needed to incorporate legal changes to remove as many barriers or delays as possible. They also mentioned that capacity-building was needed to ensure that local investigators had both the basic ability to cooperate and the human and other resources needed to do so quickly. In the view of those experts, legal provisions based on traditional physical investigative environments might need to be reconsidered, but sovereignty and jurisdiction over the physical locations where data were being stored or transmitted remained paramount. Several experts also mentioned the consideration or enactment of laws containing requirements for the localization of data that would ensure that service providers operating in their territory would be required to keep data within the territorial jurisdiction of their laws and courts, thus making extraterritorial investigative measures either unnecessary or less critical.

37. In that context, experts highlighted the importance of effective ongoing communications between States in order to share and address concerns about specific cases and increase understanding of what barriers existed and how they could be addressed. Such communications could take various forms, including the present Expert Group process, other formal or informal multilateral processes, and frequent bilateral meetings or communications. Experts noted that the views and means raised for such exchanges of information, and international cooperation in general, depended to some extent on the size and capacity of the Member States involved. That was because it was easier for larger States with more resources to post liaison personnel,

maintain channels of communication, and monitor and follow up on lessons learned. In contrast, smaller States tended to focus more on the need for multilateral processes or forums.

38. Some experts expressed the view that Member States would need to take more open approaches to sovereignty and cooperation in order to successfully address the problem of cybercrime and that, to the extent possible, "fast-track" processes were needed to make responses to cybercrime faster than those in conventional investigations. One expert noted that the draft comprehensive study had not looked at the possibility of transferring criminal proceedings and suggested that such a possibility be considered. Some experts suggested that efforts be made to reduce bureaucratic delays and streamline both formal and informal cooperation, but other experts pointed out that delays seen as bureaucratic by the requesting State were often due process procedures needed by the requested State in order to ensure that its rule-of-law and human rights requirements had been met. There was general agreement that the issue remained a very serious problem that needed continuing consideration within each State and in bilateral, regional and global terms.

39. It was noted that a partial solution to the problem of fast cross-border access to data might lie in the fact that, while accessing data involved human rights and other legal safeguards, simply compelling a company to ensure that the data were preserved might not. Experts noted that, once the data were preserved, the case was then more similar to conventional cooperation scenarios in which there was time to follow conventional mutual legal assistance and other channels. However, it was also noted that merely preserving data that would otherwise be erased might raise human rights concerns in some legal systems. One expert said that the legal system in his country allowed for such preservation and also made an exception for the immediate sharing of such non-content data as would be needed to trace communications and identify other States in time to request assistance from them before data were automatically erased. He noted that once data had been preserved and essential routing information had been shared, normal proceedings were followed to determine whether transmission of the data to the requesting State was justified.

40. Several experts also mentioned the need for standard-setting and technical assistance with respect to the collection, preservation and use of electronic evidence. They noted that both prosecutions in domestic scenarios and those carried out as a result of transnational investigations could fail if electronic evidence was not collected properly and copied and stored in ways that would meet domestic and foreign forensic standards and evidentiary requirements. Experts also raised the need for forensic standards as a possible matter for model laws, some form of specific instrument or as a possible element of a universal legal instrument. Forensic standards were also noted as an important priority for technical assistance and training.

41. A representative of the Secretariat noted that the data suggested that the majority of transnational cybercrime offences involved some form of organized criminal group, and there was discussion about the utility of the Organized Crime Convention in that context. Experts presented many points that reflected a similar discussion during the first meeting of the Expert Group, noting that the Convention could be applied in any cybercrime scenario where an organized criminal group was involved but that it did not necessarily provide for the fast responses or specialized forms of cooperation needed in respect of cybercrime.

42. There was general agreement among experts on the need to include effective prevention measures at national and international levels. The representative of the Secretariat noted that such prevention measures were also seen as important by the private sector and that companies had provided information on what they were doing or thought that they could contribute. One expert observed that responding to

cybercrime was like systems engineering in the sense that no single response would be sufficient and that it was necessary to look at the entire system and target preventive and reactive measures in different places. In that context, observations were also similar to those made at the first meeting: preventive activities included activities such as (a) raising awareness about the risks of cybercrime and the likelihood of prosecution and punishment for offenders; (b) cybersecurity measures to protect technologies and their users; and (c) efforts to prevent further crime by identifying and disrupting ongoing illicit online activities, including by taking down botnets. Other experts noted that prevention needed to involve the private sector and that it generally did not require legislation.

C. Discussion of the way forward and other matters (agenda items 5 and 6)

43. As noted in paragraph 5 above, the Expert Group could not reach consensus on any detailed substantive conclusions or recommendations on the draft comprehensive study or the way forward, apart from recommending further consideration of the study by the Commission at its twenty-second session. There was broad support among experts for technical assistance and capacity-building, but a range of views was expressed regarding whether such assistance and capacity-building could best be done under the auspices of a universal legal framework or the existing ad hoc demand-based processes. There was general agreement that more time was needed to review and discuss the text of the study in detail. Some experts, however, argued that in view of the seriousness and urgency of the problem and the lack of time and resources, the matter should be referred back to the Commission. Other experts argued that such an action was premature and that options that could not find consensus in the present Expert Group process would be unlikely to be adopted by the Commission. In the view of those experts, the mandate of the Expert Group required it to fully review the data, conclusions and findings and decide what recommendations should be transmitted. There were also divergent views on whether various options in the executive summary were viable or not, whether they were linked or could be proceeded with independently and whether alternative findings and additional options should be considered.

44. Some practical concerns were also raised with respect to a referral of the comprehensive draft study to the Commission in its present form. It was noted that owing to a lack of resources, the draft study was available in English only and could therefore not be submitted as an official document. Several experts also noted that a number of issues had been raised during the meeting and inquired whether those issues could be reflected in the text. Others pointed out that the inclusion of such issues in the text would be problematic, given the possibility of contradictory or controversial changes and lack of opportunity for the Secretariat to consult the Expert Group prior to the next session of the Commission.

45. While there was no consensus on some of the substantive issues discussed, there was general or substantial agreement on a number of key points. Most experts indicated that the text of the draft comprehensive study was a good basis for further and ongoing discussions. It was noted, however, that more time was needed to fully consider the rich volume of data collected by the Secretariat in order to examine the various interpretations and implications the study might have. There were divergent views on whether further discussions should be pursued in the context of a formal treaty-making mandate. Nevertheless, there was general agreement that cybercrime posed a serious and evolving problem, that some form of ongoing deliberations were needed and that they should take place under the auspices of the United Nations on an open-ended basis. A number of experts also noted that the problem of cybercrime

required the mobilization of a broad range of multidisciplinary expert and institutional resources, both at the national and global levels, and that such mobilization required some degree of ongoing engagement of private sector, academia and other expert resources in any continuing United Nations deliberations.

D. Adoption of the report (agenda item 7)

46. In presenting the report, the Rapporteur noted that because of the lack of resources, it was a short procedural text only. He expressed serious concern about the budgetary environment and the effects that that environment was having on the work of the Expert Group. He noted that the function of reports was to document deliberations, in order to support efforts to make processes such as the present expert study as fruitful as possible. He also noted that the functions of an intergovernmental expert process were both to develop expert opinion on matters of substance and to articulate the positions of the Member States themselves on relevant issues and options. In that context, views expressed by experts in the meetings of the Expert Group were not merely the comments on the study, but rather important elements of the study itself, representing the intergovernmental element of the process. The Rapporteur noted that, while the mandates of some of the political bodies within the United Nations might be well served by short action-oriented procedural reports, the work of substantive bodies such as the present Expert Group required substantive records of deliberations, without which important information would be lost. He expressed the view that such records were essential to inform the Commission, other convening bodies and stakeholders, and future meetings of the Expert Group itself. He also expressed the hope that substantive reports would ultimately be produced for adoption.

47. The procedural report was then adopted and the meeting was adjourned.