24 April 2017

Original: English

Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 10 to 13 April 2017

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. At that meeting, the Expert Group reviewed and adopted a collection of topics and a methodology for the study (E/CN.15/2011/19, annexes I and II).

3. The second meeting of the Expert Group was held from 25 to 28 February 2013. At that meeting, the Expert Group took note of the comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, as prepared by the United Nations Office on Drugs and Crime (UNODC) with the guidance of the Expert Group, pursuant to the mandate contained in General Assembly resolution 65/230 and the collection of topics for consideration within a comprehensive study of the impact of and response to cybercrime and the methodology for that study, as adopted at the first meeting of the Expert Group. Diverse views were expressed regarding the content, findings and options presented in the study (see UNODC/CCPCJ/EG.4/2013/3).

4. In the Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, adopted by the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice and endorsed by the General Assembly in its resolution 70/174, Member States noted the activities of the Expert Group, the international community and the private sector, and invited the Commission to consider recommending that the Expert Group continue, based on its work, to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing

responses and to propose new national and international legal or other responses to cybercrime.

II. Recommendations

5. The Commission may wish to recall General Assembly resolutions 65/230 and 70/174, and its resolutions 22/7 and 22/8, which are relevant to the work of the Expert Group.

6. The Commission may wish to request that the Expert Group continue its work and, in so doing, hold periodic meetings and function as the platform for further discussion on substantive issues on cybercrime, keeping pace with its evolving trends and, in line with the Salvador Declaration and the Doha Declaration, request the Expert Group to continue to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime. In that regard, the Commission may wish to consider exploring possibilities to provide the resources needed for the Expert Group's work.

7. The Commission may wish to decide that the Expert Group dedicate its future meetings to examining, in a structured manner, each of the main issues dealt with in chapters 3 to 8 of the draft comprehensive study, without prejudice to other issues included in the mandate of the Expert Group and taking into account, as appropriate, contributions received pursuant to its resolution 22/7 and the deliberations held at the previous meetings of the Expert Group:

- Chapter 3. Legislation and frameworks
- Chapter 4. Criminalization
- Chapter 5. Law enforcement and investigations
- Chapter 6. Electronic evidence and criminal justice
- Chapter 7. International cooperation
- Chapter 8. Prevention

8. The Commission may wish to encourage the Expert Group to develop possible conclusions and recommendations, for submission to the Commission.

9. The Commission may wish to request that UNODC periodically collect further information on developments, progress made and best practices identified.

10. The Commission may wish to invite the Expert Group to provide advice, based on its work, to UNODC, including with regard to its Global Programme on Cybercrime, in order to assist, without prejudice to other issues included in the mandate of the Expert Group, in identifying high-priority capacity-building needs and effective responses, also without prejudice to the status of the Commission as the governing body for the UNODC crime programme.

III. Summary of deliberations

A. Update by the Secretariat on the status of implementation of General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8

11. At its 1st meeting, on 10 April 2017, the Expert Group considered agenda item 2, entitled "Update by the Secretariat on the status of implementation of General Assembly resolution 65/230 and Commission on Crime Prevention and

Criminal Justice resolutions 22/7 and 22/8" (see para. 55). The Secretariat delivered an oral update on the implementation of those resolutions.

12. Many speakers expressed their appreciation for the work of the Chair and Bureau of the Expert Group and of the Secretariat in organizing and preparing for the third meeting of the Expert Group. Appreciation was also expressed for the oral report of the Secretariat under agenda item 2. With regard to the implementation of Commission resolution 22/8, many speakers welcomed the work of UNODC through its Global Programme on Cybercrime in providing technical assistance and building capacity for countering cybercrime, especially in developing countries, on the basis of the needs of requesting States, and in creating a central data repository of cybercrime laws and lessons learned. Speakers welcomed also the training activities provided to law enforcement authorities and awareness-raising activities for the public in respect of online child protection, among other things.

13. Speakers representing States that are donors of Global Programme on Cybercrime expressed their strong support for the Programme and called on other Member States to also contribute funds for technical assistance activities to combat cybercrime and for continuing the implementation of the mandates set out in Commission resolution 22/8. One speaker representing a donor State noted that his Government would likely continue to fund the programme in 2017, and requested that this updated information be reflected in the report of the Expert Group. Many speakers representing States that were recipients of technical assistance through the Global Programme also called for sustainable funding for the Programme. Some speakers stated that the technical assistance activities under the Programme should be made more transparent, inclusive and operable and information about the activities and beneficiary and requesting countries should be more readily available and shared. Many speakers emphasized that technical assistance and capacity-building activities should be carried out by UNODC in collaboration with relevant partner organizations.

14. Most speakers emphasized the necessity of achieving effective and strengthened regional and international cooperation to combat cybercrime. National legal frameworks, the capability to enforce the law and international cooperation were crucial in that regard. It was widely noted that the threat of cybercrime continued to grow and was linked to transnational organized crime and other serious crimes, terrorism, and radicalization, among other things. Among the challenges in the area of cooperation to combat cybercrime that were highlighted were the harmonization of criminalization provisions, the establishment of procedural powers for law enforcement, giving a quick response to requests for international cooperation and the issue of determining jurisdiction for the purpose of securing electronic evidence. Many speakers highlighted their Governments' responses to cybercrime and policies to prevent and combat it, which included strengthened national legal frameworks, the creation of appropriate national infrastructure, such as specialized cybercrime units and computer emergency response teams, and strengthened public-private partnerships.

15. With regard to the work of the Expert Group, several speakers expressed the hope that the Expert Group would continue to meet in the future to exchange information and discuss technical assistance, trends and developments, lessons learned and best practices among its experts in order to, among other things, support and provide substantive guidance to the work of UNODC through its Global Programme on Cybercrime and its assistance activities, and to provide assistance to Member States through its deliberations.

16. Several speakers shared their experiences in implementing the Budapest Convention on cybercrime. They stressed that that process helped them to shape national legislation and to undertake international cooperation. The same speakers indicated that the Budapest Convention was a legal instrument that was open for adherence by States outside Europe, which made it a useful international legal framework for action to combat cybercrime. Speakers also shared their experiences

related to technical assistance activities carried out under Global Action on Cybercrime, a joint project of the European Union and the Council of Europe, and in the framework of other intergovernmental organizations, such as the Organization of American States and the African Union. Other speakers noted that a strengthened international legal framework for combating cybercrime was needed. Some speakers expressed the view that the Budapest Convention was becoming outdated.

17. Several speakers noted that their Governments were carefully studying the draft comprehensive study on cybercrime. Speakers also noted that the draft study, which had been made available in 2013, was quickly becoming outdated, as it lacked data on information and communications technology that was not widely available or used at the time of its preparation, such as the Internet of things, ransomware, botnets, and tablets and smartphones. Speakers further noted that the draft study could be used as reference material in the delivery of technical assistance.

B. Adoption of the summaries by the Rapporteur of deliberations at the first and second meetings of the Expert Group

18. At its 2nd meeting, on 10 April 2017, the Expert Group considered agenda item 3, entitled “Adoption of the summaries by the Rapporteur of deliberations at the first and second meetings of the Expert Group”.

19. The Rapporteur of the Expert Group, Christopher Ram (Canada), introduced the summary reports of the 2011 and 2013 meetings of the Expert Group. He pointed out that those reports were of a substantive nature and that they supplemented the brief reports of the 2011 and 2013 meetings, which had been purely procedural due to the limited resources available at that time. The Rapporteur also explained the methodology used for the drafting of the substantive summary reports to ensure the accuracy, consistency and balance of their content, such as the use of extensive notes and the official audio recordings of the meetings, as well as continuous communication and coordination with the Secretariat.

20. The Rapporteur stressed that the substantive summary reports were significant because they documented the exchange of views about the problem of cybercrime within the Expert Group, the largest intergovernmental body in this field ever convened, and would therefore further facilitate discussions within the Expert Group at its present and future meetings, thus avoiding duplication of work. The reports themselves generally followed the agenda and structure of the two meetings, although the Rapporteur made an effort to cluster the substantive issues thematically to ensure coherence and clarity and guide future deliberations. Appropriate cross references and procedural explanations were inserted to ensure that the summary reports could be treated as stand-alone texts.

21. After the presentation by the Rapporteur, the Expert Group adopted the summary reports without further comments on their content. The Chair congratulated the Rapporteur on his work and on the very concise reports, and observed that many delegates shared that appreciation.

22. Upon conclusion of the deliberations under agenda item 3, and in line with the information provided to the extended Bureau of the Expert Group at its meeting on 15 March 2017, Erik Planken (Netherlands), nominated by Western European and other States, took up his functions as the new Rapporteur of the Expert Group.

C. Consideration of the draft comprehensive study of the problem of cybercrime and comments thereto, and consideration of the way forward on the draft study

23. At its 2nd and 3rd meetings, on 10 and 11 April 2017, respectively, the Expert Group considered agenda item 4, entitled “Consideration of the draft comprehensive

study of the problem of cybercrime and comments thereto, and consideration of the way forward on the draft study".

24. There was general agreement that the Expert Group should continue its work in the future, building on the information contained in the draft study. One delegation was of the view that the mandate of the Expert Group, as contained in General Assembly resolution 65/230, in line with the Salvador Declaration and reiterated in resolution 70/174 in which the General Assembly adopted the Doha Declaration, should be updated, while others were opposed to changing the mandate of the group.

25. Many speakers acknowledged that the text of the draft study was an amalgam of divergent views and approaches and did not represent a consensus, nor had it been negotiated to reflect a common denominator among Member States. However, speakers also stressed that the draft study was useful as a comprehensive snapshot of crime prevention and criminal justice measures against cybercrime worldwide and as a foundation for further work and exchanges of views among Member States. Some speakers were of the view that the Expert Group should take note of the content and outcome of the draft study. Other speakers preferred to delete the key findings and options and expressed concern that taking note of the text would suggest endorsement of content that was not supported by consensus in the Expert Group. Some speakers explored whether other terminology would describe follow-up action by the Expert Group more appropriately and precisely.

26. Several speakers argued that there were inconsistencies between some of the findings of the draft study and the passages substantiating those findings, or that some of the findings lacked references to proposed solutions. A common challenge identified by the majority of the speakers was the dynamic and evolving nature of cybercrime which had rendered some parts or data of the draft study outdated. Nevertheless, many speakers considered that the draft study was still relevant and that that common challenge was an opportunity to assess in depth what aspects of the draft study needed updating and what elements or parameters not reflected in the draft study could be taken into account, such as the darknet and the use of virtual currencies in criminal activities. In that regard one speaker expressed the opinion that updating the draft study or its parts would not be possible, as deliberations on the content of the draft study had already taken place during the second meeting of the Expert Group, held in 2013, and that those deliberations had been reflected in Commission resolution 22/7. According to one speaker it had to be kept in mind that the draft study was a compilation of the opinions and positions provided, in particular, by States.

27. Adopting the draft study was generally seen as not feasible due to divergent national views on some of its findings which were understood as policy recommendations. However, some speakers supported concluding and adopting the draft study at the meeting so that it could be used afterwards as reference material. They stated that any additional material brought to the attention of the Expert Group should not entail extensive redrafting of the study. Some speakers also suggested providing the Expert Group with regular budget resources within the framework of the Commission.

28. Furthermore, some speakers favoured a chapter-by-chapter approach when discussing the next steps of the Expert Group relating to the use and consideration of the draft study as a way to structure a follow-up road map and reflect on any progress made in the various areas of discussion, without redrafting the entire study.

29. There was broad support for efforts to enhance the capabilities of national authorities to deal effectively with challenges posed by cybercrime and challenges associated with electronic evidence. Many speakers highlighted the importance of exchanging information and best practices, developing and/or upgrading legislation and strengthening international cooperation mechanisms as technical assistance priorities. Several speakers supported closer coordination between the Expert Group and the UNODC Global Programme on Cybercrime in relation to capacity-building

and technical assistance issues. Some speakers referred to the added value of existing regional and international instruments as guidance frameworks for enhancing the capacity of competent authorities and the effectiveness of countermeasures in the field of cybercrime. As examples were mentioned the Budapest Convention, the African Union Convention on Cybersecurity and Personal Data Protection, the Arab Convention on Combating Information Technology Offences and the draft agreement of the Organization of Ibero-American States on the electronic transmission of requests for international cooperation among central authorities of its members.

D. Exchange of information on national legislation, best practices, technical assistance and international cooperation

30. Speakers shared information on their national laws and legislations on cybercrime, which included the criminalization of offences, such as online child abuse, fraud, forgery, identity theft, the use of malware and botnets, attacks on computer systems and networks, the illegal sale of narcotics and other illegal substances, trafficking in human organs, trafficking in human beings, especially women and children, acts of a racist or xenophobic nature, and the promotion of terrorism and extremism in cyberspace. Many speakers indicated that their legislation was aimed at striking a balance between reaping the economic and social advantages of cyberspace and related technology, while protecting their citizens and businesses. Some speakers shared examples of how long-existing laws criminalizing conventional crimes could be used to criminalize forms of cybercrime where information and communications technology enable illegal activities. Many speakers noted that they were currently in the process of updating or amending existing legislation, or introducing new laws relating to cybercrime. Some speakers noted that their countries' legislation still had gaps in relation to certain offences. Many speakers stressed the need to balance procedural powers, such as for obtaining data, with human rights considerations, including the right to privacy.

31. Many speakers noted that their national legislation was aligned with or modelled on the Budapest Convention. Those speakers represented States that were parties to the Convention, States that were not and States that were in the process of acceding. Many speakers shared information on how their Governments were transposing the Convention into their national legislation. That process included creating new criminal provisions; adopting procedures for requesting and securing electronic evidence and granting procedural powers for other purposes, taking into account human rights safeguards; and using the Convention for international cooperation, including the establishment of infrastructure, such as "24/7" networks and specialized units.

32. Speakers emphasized that international cooperation was crucial to effectively combat cybercrime given its cross-border and rapidly-evolving nature. Many speakers highlighted the need for fast and effective responses to requests for mutual legal assistance related to preserving and obtaining electronic evidence. Several speakers noted that the use of informal channels and expedited means of cooperation, such as police-to-police cooperation, were often a better alternative or a useful supplement to formal mutual legal assistance modalities, as they could ensure timely responses to urgent requests for assistance. Some speakers stated that some of the requests for mutual legal assistance issued by their Governments were not answered. Speakers noted that formal channels of international cooperation included the use of bilateral and regional treaties, the Budapest Convention and the United Nations Convention against Transnational Organized Crime. Reciprocity was also mentioned as a legal basis for mutual legal assistance in the absence of such legal instruments.

33. Many speakers highlighted the important role played by their designated central authorities and their dedicated 24/7 points of contact in receiving and processing requests for mutual legal assistance in a timely manner. Some speakers

provided examples of successful national mechanisms for responding to such requests, such as having different procedures in place for dealing with specific types of data preservation requests and mentoring requesting States on a case-by-case approach in order to expedite future requests made to the same jurisdiction.

34. Many speakers emphasized the importance of regional cooperation to combat cybercrime, including through regional frameworks and organizations such as the Inter-American Committee against Terrorism of the Organization of American States, the Common Market of the South, the Gulf Cooperation Council, the Council of Europe, the European Union, the African Union, the Association of Southeast Asian Nations and the Organization for Security and Cooperation in Europe.

35. In relation to technical assistance and capacity-building, many speakers shared their experiences of working with other States and organizations and projects such as Global Action on Cybercrime, the European Police Office and its European Cybercrime Centre, the International Criminal Police Organization, the Global Forum on Cyberexpertise, the Commonwealth, the International Telecommunication Union and UNODC. Speakers emphasized technical assistance needs and activities under way, such as training courses for police, judges and prosecutors on the handling of electronic evidence for use in investigations and prosecutions; initial assessments of countries' legislative, institutional and criminal justice frameworks and needs; assistance for States acceding to the Budapest Convention in the drafting or updating of cybercrime legislation or for creating legislation implementing that Convention; and training courses related to international cooperation and the investigation of cybercrime cases. Various speakers underlined that such technical assistance and capacity-building programmes had advanced their countries' abilities and capabilities in a relatively short period of time. For example, one speaker mentioned that, because of such advances, his country could now serve as a new hub for capacity-building in the region. The importance of cooperation among developing countries in the provision of technical assistance was also emphasized. Some speakers emphasized the need for a more balanced development and distribution of global Internet infrastructure for enhancing the capability for preventing and combating cybercrime.

36. Many speakers shared information on their national policies and strategies for preventing and countering cybercrime. In many countries those policies and strategies were included in or coordinated with national cybersecurity strategies. They included raising awareness among the general public and campaigns targeted at vulnerable groups in society, such as children and adolescents, to empower them to use information and communications technology in a safe and effective way. They also included mechanisms and structures for victim assistance, protection and compensation, as well as means for reporting crimes; effective national coordination among relevant government agencies, especially on enhancing cybersecurity; the creation of specialized cybercrime units within those countries' law enforcement agencies and judiciary, enhancing the use of digital forensics and the use of electronic evidence in investigations, prosecutions and adjudications; and a multi-stakeholder approach that included the private sector, civil society and academia. The importance of having good public-private partnerships was emphasized, especially with regard to detecting and reporting crimes, providing information on the location of suspects and victims, and providing other data as necessary. Many speakers also provided examples of past or recent cases of cybercrime investigations, including cross-border investigations and the practical use of cybercrime legislation.

37. Some speakers expressed their appreciation for the role of the Commission in strengthening international cooperation by serving as a platform for the exchange of information, best practices and lessons learned, developing effective responses and promoting relevant international instruments or standards in countering cybercrime.

38. Some speakers noted that an effective global response to cybercrime required the creation of a new legal instrument. One speaker stated that such an instrument

should address, among other things, substantive criminal law issues, guidance on international cooperation and the regulation of cross-border electronic evidence collection, while maintaining national jurisdiction and sovereignty. Other speakers stated that, based on experience, they saw no added value in having a new legal instrument and opposed the creation of one, and that starting a discussion along those lines would jeopardize current efforts to enhance legislation and build capacity. Many speakers noted that the creation of effective law enforcement and judicial capacities throughout the world was a priority for which technical assistance and capacity-building activities were crucial.

39. Some speakers expressed their support for the extension of the mandate of the Expert Group to serve as a platform for a continuing exchange of information on national legislation, best practices, technical assistance and international cooperation.

E. Examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime

40. Speakers in the Expert Group expressed diverse views on the enhancement of existing legal instruments and on the possibility of developing new international legal instruments on cybercrime.

41. Many speakers expressed the view that a new legal instrument on cybercrime was not needed or that the elaboration of such an instrument was not feasible. Some speakers were of the view that existing international legal instruments such as the Organized Crime Convention and the Budapest Convention could be used to develop national legislation and engage in international cooperation in the area of cybercrime. They highlighted the usefulness of the Budapest Convention for strengthening national cybercrime legislation, for both parties and others for whom that Convention served as a reference. Speakers also stated that the Budapest Convention provided an effective legal and operational framework to address cybercrime, including by facilitating international cooperation and harmonization. Speakers further stated that the flexibility and adaptability of the Convention, owing to, inter alia, its technology-neutral language and the fact that all States had the possibility to accede, contributed to its validity and usefulness. Speakers mentioned the work of the Cybercrime Convention Committee in facilitating the effective use and implementation of the Convention and the exchange of information between parties. Speakers noted the growing membership of the Committee, which included a number of parties that were not members of the Council of Europe.

42. Many speakers noted that the Budapest Convention was successful because of the capacity-building and technical assistance programmes that facilitated its implementation, including through the adoption and implementation of national legislation and the building of national capacities for investigations, prosecutions and adjudications, and international cooperation. Some speakers stated that the process of negotiating and ratifying a new legal instrument would take up valuable time and resources, which would undermine current efforts to address cybercrime.

43. Some speakers expressed support for the substantive content of the Budapest Convention but were concerned about the accession procedure, including the fact that the Convention was open for accession by invitation only, subject to the approval of its States parties. Other speakers acknowledged the value and usefulness of the Budapest Convention for countering cybercrime, but regarded it as a regional rather than an international legal instrument, in part because it had been negotiated at the regional level. Some speakers underlined that countries that were not members of the Council of Europe also participated in the negotiations. One speaker emphasized that the United Nations was the legitimate forum for the negotiation of a global legal framework and that a multilateral instrument on cybercrime would not be detrimental to existing regional instruments.

44. Some speakers expressed the need for a new legal instrument on cybercrime within the framework of the United Nations. According to those speakers, such a legal instrument could address, among other things, concerns related to cross-border data access and matters of jurisdiction, territorial integrity and national sovereignty. Some speakers were of the opinion that the Budapest Convention, in particular its article 32 (b), presented challenges relating to sovereignty. One speaker emphasized that every State considering becoming a party to the Budapest Convention had to take an informed decision with regard to the degree of national sovereignty that it was prepared to cede in favour of the other parties to the Convention. Some speakers stated that, although the Budapest Convention needed to be updated, elements could serve as a good reference for a new legal instrument. One speaker stated that it was not reasonable to object to the development of a global instrument because of the existence of a regional treaty. Many speakers underlined that the Budapest Convention was constantly kept up to date through guidance notes and, where necessary, new protocols.

45. Speakers provided their views on the draft comprehensive study on cybercrime. Many speakers stated that they could not support the current key findings and options, as these were not properly substantiated by the data and research in the draft study. Some speakers referred to written comments on the draft study provided by Member States pursuant to Commission resolution 22/7. They also noted developments since 2013 that had not been taken into account in the draft study. Several speakers stated that the key findings and options focused too much on new legal frameworks, as opposed to existing instruments, and that insufficient attention was paid to the importance of technical assistance and capacity-building. Several speakers noted that the deliberations held during the third meeting of the Expert Group had demonstrated that the findings were not considered sufficiently accurate. Some speakers indicated that they would favour the removal of the key findings and options from the text of the draft study. Other speakers indicated that they preferred not to change the key findings and options, nor to remove them. In that regard, reference was made to Commission resolution 22/7. One speaker expressed the opinion that, thus, the study was no longer a draft. The view was once again expressed that the draft study was not a negotiated document and that it could therefore not be subjected to any alterations by the Expert Group. Some speakers stated that the drafting and inclusion in the draft study of key findings and options by the authors of the draft study went beyond the mandate. Those speakers also stated that it should be the Expert Group itself that should formulate the key findings and options and that the mandate of the Expert Group should be extended through the Commission.

46. Several options were presented regarding the way forward. Several speakers suggested examining the draft study chapter by chapter at future meetings of the Expert Group. Doing so would enable the Expert Group to determine how the draft study could be improved or updated to include recent developments, such as the increased use of the darknet and of cryptocurrencies, and to arrive at key findings and options and at possible solutions to the challenges identified. Some speakers suggested that the draft study could be used as a basis or as guidance for future Expert Group discussions. Doing so would enable the Expert Group to identify the areas of priority for tackling cybercrime. It was also stated that a thorough review of the areas discussed in the draft study would, inter alia, help to identify whether a new legal instrument was needed and what such an instrument would need to address.

47. Some speakers stressed that the Expert Group would need to decide on a clear methodology and structure for its future meetings. Possible topics for future Expert Group discussions included cloud computing and cross-border access to data, encryption and forensic capacities.

48. The Expert Group reached a consensus on recommendations to the Commission regarding the future work of the Expert Group.

49. Several speakers expressed their ongoing support for the activities of UNODC, through its Global Programme on Cybercrime, in providing technical assistance and capacity-building to developing countries, and urged continued support from donors.

50. The Expert Group expressed its appreciation to the Government of China for providing extrabudgetary resources towards the holding of the third meeting of its Expert Group.

F. Other matters

51. No matters were raised under agenda item 7, “Other matters”.

III. Organization of the meeting

A. Opening of the meeting

52. The meeting was opened, on an exceptional basis, by the Permanent Representative of South Africa to the United Nations on behalf of the Chair of the Expert Group, as the Chair was indisposed and no Vice-Chairs were available.

B. Statements

53. Statements were made by experts of the following States: Algeria, Argentina, Australia, Belarus, Belgium, Brazil, Canada, Chile, China, Colombia, Côte d’Ivoire, Croatia, Czechia, Dominican Republic, Ecuador, Egypt, El Salvador, Estonia, Finland, France, Georgia, Germany, Ghana, Guatemala, Hungary, India, Iran (Islamic Republic of), Italy, Japan, Kenya, Kuwait, Malta, Mexico, Morocco, Netherlands, Norway, Oman, Pakistan, Peru, Philippines, Portugal, Republic of Korea, Republic of Moldova, Romania, Russian Federation, Saudi Arabia, Senegal, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Sudan, Turkey, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay and Viet Nam.

54. Statements were also made by the representative of Malta on behalf of the States Members of the United Nations that are members of the European Union.

55. In addition, statements were made by the representatives of the European Union and the Council of Europe.

C. Adoption of the agenda and other organizational matters

56. At the meeting of its extended Bureau on 15 March 2017, the Expert Group adopted the following provisional agenda:

1. Organizational matters:
   (a) Opening of the meeting;
   (b) Adoption of the agenda.
2. Update by the Secretariat on the status of implementation of General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8.
3. Adoption of the summaries by the Rapporteur of deliberations at the first and second meetings of the Expert Group.
4. Consideration of the draft comprehensive study of the problem of cybercrime and comments thereto, and consideration of the way forward on the draft study.

5. Exchange of information:

   (a) National legislation;

   (b) Best practices;

   (c) Technical assistance;

   (d) International cooperation.

6. Examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime.

7. Other matters.

8. Adoption of the report.

D. Attendance

57. The meeting was attended by representatives of 87 Member States, 4 intergovernmental organizations, 2 institutions from academia and 1 from the private sector.

58. A list of participants was circulated at the meeting (UNODC/CCPCJ/EG.4/2017/INF/1).

E. Documentation

59. In addition to the draft comprehensive study of the problem of cybercrime and responses to it from Member States, the international community and the private sector, the Expert Group had before it the following documents:

(a) Provisional agenda (UNODC/CCPCJ/EG.4/2017/1/Rev.1);

(b) Summary by the Rapporteur of 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 (UNODC/CCPCJ/EG.4/2017/2);

(c) Summary by the Rapporteur of 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 (UNODC/CCPCJ/EG.4/2017/3);

(d) Note by the Secretariat regarding information on the implementation of Crime Commission resolution 22/8 (UNODC/CCPC/EG.4/2017/CRP.1);

(e) Non-paper submitted by the European Union on capacity-building on cybercrime and e-evidence: the experience of joint projects of the European Union and the Council of Europe, 2013-2017 (UNODC/CCPC/EG.4/2017/CRP.2).

IV. Adoption of the report

60. At its 7th meeting, on 13 April 2017, the Expert Group adopted its report (UNODC/CCPCJ/EG.4/2017/L.1 and Add.1 to 4).