Distr.: General
12 April 2019

Original: English

Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019

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 in Vienna 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 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 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.

5. The third meeting of the Expert Group was held in Vienna from 10 to 13 April 2017. At that meeting, the Expert Group considered, inter alia, the adoption of the summaries by the Rapporteur of deliberations at the first and second meetings of the Expert Group, the draft comprehensive study of the problem of cybercrime and comments thereon and the way forward on the draft study. It also exchanged information on national legislation, best practices, technical assistance and international cooperation.

6. In its resolution 26/4, adopted at its twenty-sixth session in May 2017, the Commission requested the Expert Group to continue its work and, in so doing, to hold periodic meetings and function as the platform for further discussion on substantive issues concerning cybercrime, keeping pace with its evolving trends, and in line with the Salvador Declaration and the Doha Declaration. Also in that resolution, the Commission requested 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 propose new national and international legal or other responses to cybercrime.

7. The fourth meeting of the Expert Group was held in Vienna from 3 to 5 April 2018. At that meeting, the Expert Group focused on legislation and frameworks and criminalization related to cybercrime. Legislative and policy developments with regard to addressing cybercrime at the national and international levels were discussed and consideration was given to the ways in which cybercrime was criminalized at the national level. The Expert Group also adopted the Chair's proposal for the workplan of the Expert Group for the period 2018–2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. The dates for the fifth meeting of the Expert Group were decided and the provisional agenda agreed upon by the extended Bureau at its meeting on 2 November 2018.

II. List of preliminary recommendations and conclusions

9. In line with the workplan of the Expert Group for the period 2018–2021, the Rapporteur will prepare, at each of the meetings of the Expert Group in 2019 and 2020, with the assistance of the Secretariat and on the basis of the discussions and deliberations of the Expert Group, a list of preliminary conclusions and recommendations suggested by Member States that should be precise and should focus on strengthening practical responses to cybercrime. Pursuant to the workplan, that list will be included in the report of each meeting in the form of a compilation of suggestions made by Member States, to be discussed further at the stock-taking meeting to be held no later than 2021. As specified in the workplan, at that stock-taking meeting, the Expert Group will consider the preliminary conclusions and recommendations and consolidate them in a list of adopted conclusions and recommendations for submission to the Commission. Prior to the stock-taking meeting, the preliminary conclusions and recommendations proposed by Member States will be circulated to all Member States, observers and other stakeholders for comments, which will then be posted online in advance of the stock-taking meeting for consideration by delegations.

A. Law enforcement and investigations

10. In line with the workplan, the present paragraph contains a compilation of suggestions made by Member States at the meeting under agenda item 2, entitled "Law enforcement and investigations". These preliminary recommendations and

conclusions were submitted by Member States and their inclusion does not imply their endorsement by the Expert Group, nor are they listed in order of importance:

(a) Some Member States suggested that owing to the evolving, complicated and transnational nature of cybercrime, it would be premature to discuss common standards in international cooperation. Therefore, Member States should pursue new international responses against cybercrime by considering the negotiation of a new global legal instrument on cybercrime within the framework of the United Nations. That instrument should be considered taking into account, inter alia, the concerns and interests of all Member States and the proposed draft United Nations convention on cooperation in combating cybercrime submitted to the Secretary-General on 11 October 2017 (A/C.3/72/12, annex);

(b) However, other Member States suggested that it was not necessary or appropriate to consider a new global legal instrument because the challenges posed in respect of cybercrime and the sufficient training of investigators, prosecutors and judges were best addressed through capacity-building, active dialogue and cooperation among law enforcement agencies and the use of existing tools, such as the Council of Europe Convention on Cybercrime (Budapest Convention). On the basis of that suggestion, Member States should continue to use and/or join existing multilateral legal instruments on cybercrime such as the Budapest Convention, which is considered by many States to be the most relevant guide for developing appropriate domestic legislation – of both a substantive and procedural nature – on cybercrime and facilitating international cooperation to combat such crime;

(c) In view of the transnational nature of cybercrime and the fact that the large majority of global cybercrimes are committed by organized groups, Member States should also make greater use of the United Nations Convention against Transnational Organized Crime to facilitate the sharing of information and evidence for criminal investigations relating to cybercrime;

(d) Member States should promote and engage in international cooperation to combat cybercrime, making use of existing instruments, concluding bilateral agreements based on the principle of reciprocity and supporting, in collaboration with UNODC, regular networking and information-sharing among judicial and law enforcement authorities;

(e) Countries should develop the expertise of police officers in investigating cybercrime by providing them with training, which is offered by numerous countries as well as by UNODC and other partners and is intended to strengthen capacities to detect, investigate and fight cybercrime. Capacity-building in that area should, in particular, address the needs of developing countries, focus on the vulnerabilities of each country in order to provide tailor-made technical assistance and promote the exchange of the most up-to-date knowledge in the best interests of the beneficiaries;

(f) States are encouraged to continue to provide UNODC with the necessary mandates and financial support with a view to delivering tangible results in capacity-building projects in that area;

(g) Countries should devote resources to developing expertise to investigate cybercrime and to creating partnerships that employ cooperation mechanisms to obtain vital evidence;

(h) Member States should continue their efforts to develop and support specialized cybercrime units, bodies and structures within law enforcement and prosecution authorities and the judiciary, so that they have the necessary expertise and equipment to address the challenges posed by cybercrime and for the gathering, sharing and use of electronic evidence in criminal proceedings;

(i) Given that cybercrime requires medium- and long-term law enforcement strategies to disrupt cybercrime markets, including cooperation with international partners, those strategies should be proactive and preferably target organized cybercriminal groups, which may have members in numerous countries;

(j) Countries should continue to enact substantive legislation on new and emerging forms of crime in cyberspace using technologically neutral language in order to ensure compatibility with future developments in the field of information and communications technologies;

(k) Domestic procedural laws must keep pace with technological advances and ensure that law enforcement authorities are adequately equipped to combat online crime. Relevant laws should be drafted taking into account applicable technical concepts and the practical needs of cybercrime investigators, consistent with due process guarantees, privacy interests, civil liberties and human rights, as well as the principles of proportionality and subsidiarity and safeguards ensuring judicial oversight. Moreover, Member States should devote resources to enacting domestic legislation that authorizes:

(i) Requests for the expedited preservation of computer data to the person in control of the data – that is, Internet and communications service providers – to keep and maintain the integrity of those data for a specified period of time owing to their potential volatility;

(ii) The search and seizure of stored data from digital devices, which are often the most relevant evidence of an electronic crime;

(iii) Orders to produce computer data that may have less privacy protection, such as traffic data and subscriber data;

(iv) The real-time collection of traffic data and content in appropriate cases;

(v) International cooperation by domestic law enforcement authorities;

(l) As cybercrime investigations require creativity, technical acumen and joint efforts between prosecutors and the police, countries should encourage close cooperation between public prosecutors and the police at an early stage in an investigation in order to develop sufficient evidence to bring charges against identified subjects;

(m) Law enforcement officers should be guided by investigators when conducting investigations into cybercrime cases to ensure that due process standards are respected;

(n) Domestic law enforcement agencies should reach out to and engage with domestic Internet service providers and other private industry groups. This outreach supports law enforcement investigations by increasing trust and cooperation among stakeholders;

(o) Countries should adopt flexible approaches to applicable jurisdictional bases in the field of cybercrime, including greater reliance on the location from which information and communications technology services are offered rather than on the location where data reside;

(p) Countries should invest in raising awareness of cybercrime among the general public and private industry in order to address the lower rates of reporting of cybercrime compared with other types of crime;

(q) Member States should foster public-private partnerships to combat cybercrime, including through the enactment of legislation and the establishment of channels for dialogue for that purpose, in order to promote cooperation between law enforcement authorities, communication service providers and academia with a view to enhancing knowledge and strengthening the effectiveness of responses to cybercrime;

(r) States should take measures to encourage Internet service providers to play a role in preventing cybercrime and supporting law enforcement and investigation activities, including by establishing in their domestic legislation relevant provisions on the obligations of those service providers, and clearly define the scope and

boundary of such obligations in order to protect the legitimate rights and interests of service providers;

(s) States should strengthen investigation and law enforcement activities related to the acts of aiding, abetting and preparing cybercrime, with a view to effectively addressing the complete chain of cybercrime;

(t) States should continue to strengthen capacity-building and enhance the capability of the judicial and law enforcement authorities in investigating and prosecuting cybercrime. The increasing challenges posed by cloud computing, the darknet and other emerging technologies should be emphasized in capacity-building activities. Moreover, States are encouraged to provide capacity-building assistance to developing countries.

B. Electronic evidence and criminal justice

11. In line with the workplan, the present paragraph contains a compilation of suggestions made by Member States at the meeting under agenda item 3 entitled "Electronic evidence and criminal justice". These preliminary recommendations and conclusions were submitted by Member States and their inclusion does not imply their endorsement by the Expert Group, nor are they listed in order of importance:

(a) Member States should develop and implement legal powers, jurisdictional rules and other procedural provisions to ensure that cybercrime and crimes facilitated by the use of technology can be effectively investigated at the national level and that effective cooperation can be achieved in transnational cases, taking into account the need for effective law enforcement, national sovereignty and the protection of privacy and other human rights. This may include:

(i) The adjustment of rules of evidence to ensure that electronic evidence can be collected, preserved, authenticated and used in criminal proceedings;

(ii) The adoption of provisions on the national and international tracing of communications;

(iii) The adoption of provisions governing the conduct of domestic and cross-border searches;

(iv) The adoption of provisions on the interception of communications transmitted via computer networks and similar media;

(v) The enactment of substantial and procedural laws that are technologically neutral to enable countries to tackle new and emerging forms of cybercrime;

(vi) The harmonization of national legislation;

(vii) The enactment of new or strengthening of existing legislation to make it possible to recognize the admissibility of electronic evidence and define and establish the scope of electronic evidence;

(b) Member States should foster efforts to build the capacity of law enforcement personnel, including those working in specialized law enforcement structures, prosecutors and the judiciary, so that such personnel possess at least basic technical knowledge of electronic evidence and are able to respond effectively and expeditiously to requests for assistance in the tracing of communications and undertake other measures necessary for the investigation of cybercrime;

(c) Member States should foster capacity-building in order to improve investigations, increase understanding of cybercrime and the equipment and technologies available to fight it and enable prosecutors, judges and central national authorities to appropriately prosecute and adjudicate on such crime;

(d) Member States should foster efforts to build the capacity of central authorities involved in international cooperation on requirements and procedures

relating to mutual legal assistance, including by providing training on the drafting of comprehensive requests with sufficient information for obtaining electronic evidence;

(e) Member States should consider the "prosecution team" approach, which combines the skills and resources of various agencies, bringing together prosecutors, investigative agents and forensic analysts to conduct investigations. That approach allows prosecutors to handle and present electronic evidence;

(f) The admissibility of electronic evidence should not depend on whether evidence was collected from outside a country's jurisdiction, provided that the reliability of the evidence is not impaired and the evidence is lawfully collected, for example, pursuant to a mutual legal assistance treaty or, multilateral agreement, or in cooperation with the country that has jurisdiction;

(g) Member States should take necessary measures to enact legislation that ensures the admissibility of electronic evidence, bearing in mind that admissibility of evidence, including electronic evidence, is an issue that each country should address according to its domestic law;

(h) Member States should enhance international cooperation among law enforcement agencies, prosecutors, judicial authorities and Internet service providers in order to bridge the gap between the speed at which cybercriminals operate and the swiftness of law enforcement responses. In doing so, Member States should utilize existing frameworks, such as 24/7 networks and cooperation through the International Criminal Police Organization (INTERPOL), as well as mutual legal assistance treaties, to foster international cooperation involving electronic evidence. Member States should further harmonize and streamline processes related to mutual legal assistance and develop a common template to expedite such processes for the timely collection and transfer of cross-border electronic evidence;

(i) Member States are encouraged to increase their sharing of experiences and information, including national legislation, national procedures, best practices on cross-border cybercrime investigations, information on organized criminal groups and the techniques and methodology used by those groups;

(j) Member States should develop a network of focal points between law enforcement agencies, judicial authorities and prosecutors;

(k) Member States should evaluate the possibility of mandating the Expert Group or UNODC experts to conduct, with the contribution of Member States, an annual assessment of cybercrime trends and new threats, and to make it publicly available;

(l) UNODC should support the expansion of research activities to identify new forms and patterns of offending, the effects of offending in key areas and developments in the telecommunications environment, including the expansion of the Internet of things, the adoption of blockchain technologies and cryptocurrencies and the use of artificial intelligence in conjunction with machine learning;

(m) Through the Global Programme on Cybercrime, UNODC should promote, support and implement, as appropriate, technical cooperation and assistance projects, subject to the availability of resources. Such projects would bring together experts in crime prevention, computer security, legislation, prosecution, investigative techniques and related matters with States seeking information or assistance in those areas;

(n) UNODC should establish an educational programme focused on raising knowledge and awareness of measures to counter cybercrime, especially in the sphere of electronic evidence gathering, for the judicial and prosecution authorities of Member States;

(o) Member States should pursue action to enhance cooperation in gathering electronic evidence, including the following:

(i) Sharing of information on cybercrime threats;

(ii) Sharing of information on organized cybercriminal groups, including the techniques and methodology they use;

(iii) Fostering of enhanced cooperation and coordination among law enforcement agencies, prosecutors and judicial authorities;

(iv) Sharing of national strategies and initiatives to tackle cybercrime, including national legislation and procedures to bring cybercriminals to justice;

(v) Sharing of best practices and experiences related to the cross-border investigation of cybercrime;

(vi) Development of a network of contact points between law enforcement authorities, judicial authorities and prosecutors;

(vii) Harmonization and streamlining of processes relating to mutual legal assistance and development of a common template to expedite the process for the timely collection and transfer of cross-border electronic evidence;

(viii) Holding of workshops and seminars to strengthen the capacity of law enforcement authorities and judicial authorities for drafting requests, in the context of mutual legal assistance treaties, to collect evidence in matters related to cybercrime;

(ix) Development of standards and uniformity in procedural aspects relating to the collection and transfer of digital evidence;

(x) Development of a common approach to information-sharing arrangements with service providers in relation to cybercrime investigations and the gathering of evidence;

(xi) Engagement with service providers through public-private partnerships in order to establish modalities of cooperation in law enforcement, cybercrime investigations and evidence collection;

(xii) Development of guidelines for service providers to assist law enforcement agencies in cybercrime investigations, including with regard to the format and duration of preservation of digital evidence and information;

(xiii) Strengthening of the technical and legal capacities of law enforcement agencies, judges and prosecutors through capacity-building and skill development programmes;

(xiv) Provision of assistance to developing countries in strengthening cyber forensic capabilities, including through the establishment of cyber forensic laboratories;

(xv) Holding of workshops and seminars to raise awareness of best practices in addressing cybercrime;

(xvi) Establishment of an international agency to validate and certify digital forensics tools, preparation of manuals and strengthening of the capacity of law enforcement and judicial responses to cybercrime;

(p) Countries should invest in building and enhancing digital forensics capabilities, including training and security certifications, as well as information security management systems to support successful cybercrime prosecutions through the examination of electronic devices in order to collect evidence in a reliable manner;

(q) In legal systems that use the inquisitorial model, where judicial officers are also investigators, the judiciary should receive specialized training on cybercrime;

(r) Some judges are unfamiliar with digital evidence and as a result, this type of evidence is often subject to higher standards with regard to authentication and admission. However, consideration should be given to the fact that there is no practical reason to impose higher standards in relation to the integrity of digital evidence in contrast to traditional evidence. Digital evidence is no more likely to be

altered or fabricated than other evidence. Indeed, it is arguably harder to alter or fabricate digital evidence because various mathematical algorithms, such as “hash values”, can be used to authenticate or provide evidence of an alteration;

(s) States should improve the effectiveness of domestic inter-agency coordination and synergies, including the sharing of trusted information and intelligence, with the private sector, civil society organizations and other stakeholders to facilitate efficient international cooperation and collaboration;

(t) States should enact new or strengthen existing legislation to make it possible to recognize the admissibility of electronic evidence and define and establish the scope of electronic evidence;

(u) States may consider establishing the following data as electronic evidence in their domestic legislation: traffic data, such as log files; content data, such as emails; subscriber data, such as user registration information; and other data that are stored, processed and transmitted in a digital format and that are produced during the commission of a crime and can therefore be used to prove the facts of that crime;

(v) States are encouraged to strengthen capacity-building for the collection of electronic evidence, create professional teams equipped with both legal and technical expertise and enhance experience-sharing and training cooperation in that regard. UNODC is encouraged to play a role in those efforts;

(w) States are encouraged to establish in their domestic legislation relevant methods for collecting electronic evidence, such as the seizure and preservation of the original storage medium, on-site collection, remote collection and verification. Member States are encouraged to freeze electronic evidence to prevent addition, deletion or modification through measures such as the computation of the checksum of electronic evidence, locking of web application accounts and adoption of write protection;

(x) States are encouraged to establish technical norms and standards for the collection of electronic evidence;

(y) States should ensure that the collection of electronic evidence is in compliance with due process;

(z) States should establish rules for assessing the authenticity, integrity, legality and relevance of electronic evidence in their domestic legislation and take into account the unique characteristics of electronic evidence when applying the rules on original evidence, hearsay and the exclusion of illegal evidence;

(aa) When collecting electronic evidence abroad, States should respect the sovereignty of the States where data are located, comply with due process and respect the legitimate rights of relevant persons and entities. States should also refrain from the unilateral use of intrusive or destructive technical investigative measures in this regard;

(bb) States are encouraged to consult with other States in order to further improve international judicial assistance and enforcement cooperation by optimizing relevant procedures and methods, so as to facilitate the investigation of cybercrime and the collection of electronic evidence;

(cc) States should consider adopting international model provisions on investigative powers relating to the collection of electronic evidence and explore the possibility of negotiating a global binding instrument on combating cybercrime within the framework of the United Nations. That instrument may include universally accepted provisions on the cross-border collection of electronic evidence.

III. Summary of deliberations

A. Law enforcement and investigations

12. At its 1st, 2nd and 3rd meetings, on 27 and 28 March 2019, the Expert Group considered agenda item 2, entitled “Law enforcement and investigations”.

13. The discussion was facilitated by the following panellists: Mr. Shenkuo Wu (China); Ms. Ioana Albani (Romania); Mr. Martin Gershanik (Argentina); Mr. Pedro Verdelho (Portugal); and Mr. Anton Kurdyukov (Russian Federation).

14. During the subsequent debate, the Expert Group considered examples of alleged criminal activities carried out in the digital environment and posing significant difficulties to criminal justice practitioners and investigators in the opening and conduct of investigations and subsequent prosecutions. Such examples included online fraud, the use of the Internet for terrorist purposes, the use of the darknet to engage in illegal activities and the sexual abuse and exploitation of children through the misuse of information and communications technologies. In addition, the Expert Group was informed about the conceptual interdependence of, and distinctions between, cybercrime and cybersecurity, as well as trends and challenges pertaining to cybercrime, including ransomware attacks; social engineering tactics used to commit fraud (phishing, spear phishing, vishing, smishing); the use of the Cobalt Strike platform to carry out attacks against banking systems; the Internet of things; cryptocurrency mining and cryptojacking; and skimming and associated crimes.

15. The topic of whether a comprehensive global legal instrument on cybercrime was needed or whether States should instead focus on effectively implementing existing instruments, including the Budapest Convention, was once again discussed. Some speakers argued that additional legal instruments on cybercrime were not needed, given that the Budapest Convention provided an adequate framework for developing appropriate domestic and international responses to cybercrime. It was noted that 63 States parties had acceded to the Budapest Convention, thereby demonstrating that it was open to accession by non-members of the Council of Europe. Furthermore, it was noted that the Convention was used by some States that were not parties to it as a source of inspiration for harmonized domestic legislative standards of both a substantive and procedural nature. It was also noted that the concept of “harmonization of national standards” included not only cases of convergence and common definitions, but also cases where international norms were useful for the development of national regulations. The complementarity of the Budapest Convention with other regional instruments, such as the African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014, and the International Code of Conduct for Information Security, issued by the Shanghai Cooperation Organization, were mentioned.

16. However, other speakers argued that a global legal instrument on cybercrime within the framework of the United Nations was needed to address challenges posed by the rapid development of Internet technology that were not covered by existing mechanisms to which, moreover, not all States were parties. It was highlighted that such an instrument was envisaged as part of a United Nations-led process in which all Member States could take ownership of and responsibility for streamlined efforts towards global responses to cybercrime, taking stock of or building upon existing instruments such as the Budapest Convention and the aforementioned African Union Convention. In that context, reference was made to General Assembly resolution 73/187 of 17 December 2018 on countering the use of information and communications technologies for criminal purposes and the mandate contained therein for the Secretary-General to seek the views of Member States on the challenges that they faced in countering the use of information and communications technologies for criminal purposes, and to present a report based on those views for consideration by the General Assembly at its seventy-fourth session. The view was also expressed that the Budapest Convention was not sufficiently transparent or

inclusive, failed to address the concerns of all Member States and established complex and non-transparent processes for the amendment of its text, which could be a disadvantage in view of the constantly evolving nature of cybercrime.

17. Reference was made to the ongoing negotiation process for the adoption of a second additional protocol to the Budapest Convention aimed at providing clear rules and more effective procedures in relation to some or all of the following issues: provisions on more effective and expeditious international cooperation; provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests and emergency requests; and a framework and strong safeguards for practices involving cross-border access to data, including data protection requirements.

18. It was also stressed that the Organized Crime Convention could be a useful tool with which to address the challenges posed by cybercrime, particularly in view of the transnational nature of those challenges. A proposal was made to consider the negotiation of an additional protocol to the Organized Crime Convention that dealt specifically with cybercrime.

19. The Expert Group was informed by delegations and panellists about successful national efforts to implement legal and procedural measures to tackle cybercrime. For some speakers, the Budapest Convention and the accompanying capacity-building projects were essential building blocks in that field. The issue of legislative reform at the national level was considered thoroughly, including the scope of such reform. Attention was drawn to the need for inclusive and participatory processes to ensure that the voices of different stakeholders were taken into account. Reference was made to the need to ensure legal certainty and clarity based on the principle of *nullum crimen nulla poena sine lege* and the need to use technologically neutral language in new legislation so that such legislation would remain compatible with rapid developments in the field of information and communications technologies.

20. Discussion also revolved around challenges arising from conflicts regarding territorial jurisdiction, especially where, for example, a service provider might have its headquarters in one jurisdiction while the data controller was located in another country or the data were stored in another or in multiple jurisdictions. It was noted that the advent of cloud computing raised additional practical and legal challenges for criminal investigations. It was also noted that flexible approaches to applicable jurisdictional bases in the field of cybercrime might be useful, including greater reliance on the location from which information and communications technology services were offered rather than on the location where data were residing.

21. The Expert Group also highlighted the need for appropriate procedural powers to obtain electronic evidence, including data and metadata for investigations relating to not only cybercrime but also other forms of crime. Such electronic evidence might include subscriber information, content data or traffic data. It was noted that new technological developments such as anonymization software, high-grade encryption and virtual currencies were encountered when investigating offences involving electronic evidence, and that investigators might need to adopt new strategies and consider how to use special investigative techniques and remote digital forensics for gathering such electronic evidence while ensuring the admissibility and use of such evidence in court. Priority was accorded to enhancing the coordination role of competent national authorities such as general attorneys or specialized prosecutors' offices.

22. The discussion also focused on how to strike a balance between the need for effective law enforcement responses to cybercrime and the protection of fundamental human rights, in particular, the right to privacy. Data retention regulations might represent a pragmatic approach to ensuring that communication service providers were able to play a greater role in addressing cybercrime through enhanced cooperation with law enforcement, on the condition that such laws were implemented with due procedural safeguards and privacy protections. Reference was made to the report of the Office of the High Commissioner for Human Rights on the right to

privacy in the digital age (A/HRC/27/37), which was submitted to the Council of Human Rights in accordance with General Assembly resolution 68/167.

23. The Expert Group reiterated the importance of international cooperation in the cross-border investigation and prosecution of cybercrime. Some speakers noted that the number of requests for mutual legal assistance to obtain and preserve electronic evidence was growing fast and that traditional modalities of cooperation, especially what were considered by some to be lengthy processes related to mutual legal assistance, did not facilitate rapid access to data. Others noted that mutual legal assistance remained a critical tool for sharing data across borders. It was also noted by some speakers that capacity-building and training on requirements related to mutual legal assistance, including the drafting of comprehensive requests with sufficient information for obtaining electronic evidence, were key components for ensuring timely access to data. In addition, some countries recommended the use of 24/7 networks to request the prompt preservation of data owing to the volatile nature of such evidence, which could be transferred or deleted at the click of a mouse.

24. Different practices were mentioned as examples of how to foster international cooperation in relation to electronic evidence, in particular, at the operational level. Those practices included the direct transmission of requests for mutual legal assistance between the competent authorities of the cooperating States; the more frequent use of tailor-made international cooperation tools to safeguard the integrity of electronic evidence such as the expedited preservation of computer data; joint investigations; the use of electronic means to transmit requests for mutual legal assistance, with specific reference to the potential utility of the INTERPOL initiative on the secure electronic transmission of mutual legal assistance exchanges; the sharing of information among contact points of the 24/7 network; and the more frequent use of police-to-police cooperation, including through the assistance of INTERPOL, for the purposes of intelligence gathering. Reference was also made to the European Cybercrime Centre, which was set up by the European Union Agency for Law Enforcement Cooperation in 2013 to strengthen law enforcement responses to cybercrime within the European Union.

25. The Expert Group also touched upon the issue of cross-border access to data. Overall, it was noted that the practices and procedures used by States and the conditions and safeguards related to those practices and procedures varied considerably. Concerns were raised over the potential legal problems caused by certain practices in relation to cross-border access to data. Furthermore, emphasis was placed on the procedural rights of suspects, privacy considerations and the protection of personal data, the methods and legality of accessing data stored in another jurisdiction and respect for the principle of national sovereignty.

26. The Expert Group stressed the importance of sustainable capacity-building for enhancing the effectiveness and skills of all actors at the operational level to address the challenges posed by cybercrime. In that context, speakers referred to the usefulness of sharing good practices and experiences among practitioners, not only within but also between States. Some speakers referred to enhanced training and capacity-building in conjunction with the development of specialized cybercrime structures or units within prosecution services and law enforcement authorities. In that connection, it was stressed that, as electronic evidence had become increasingly common in the investigation of other forms of crime, it was essential to put in place specialized structures offering specific expertise, knowledge and operational skills for the investigation of those crimes.

27. The Expert Group further discussed the importance of fostering and strengthening cooperation between national authorities and the private sector, in particular, communication service providers and Internet service providers, in order to enhance the preservation of, and access to, data. While the increasing importance of such cooperation at the domestic level, especially in emergency circumstances involving serious crimes, was highlighted, it was also acknowledged that greater efforts were needed to ensure a similar level of cooperation in transnational cases. In

that regard, reference was made to the risk of conflicting requirements for communication service providers and Internet service providers, namely, how to balance their responses in view of the legal requirements of the States involved.

28. Many speakers reported on national measures to develop and implement cybersecurity strategies and policies; enact and/or upgrade legislation on cybercrime; implement new investigative tools to gather electronic evidence and establish its authenticity for evidentiary purposes in criminal proceedings, taking into account human rights safeguards; implement institutional arrangements geared towards ensuring the more efficient use of resources to combat cybercrime; and promote international cooperation to combat cybercrime. One speaker said that the differences between cybersecurity and cybercrime were the main consideration when structuring domestic responses and defining institutional competences on those matters.

29. Many speakers supported the work of the Expert Group as the only comprehensive – and the most appropriate – global forum for facilitating discussion and exchanges of views among Member States on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen national and international legal and other responses to cybercrime. The value added by the Commission in that regard was also mentioned. It was stated that the Expert Group had a unique mandate to act as a platform for discussions on the topic; however, that would not necessarily exclude other initiatives aimed at developing comprehensive global governance to combat cybercrime.

30. Support was expressed for the work carried out by UNODC in the areas of technical assistance and capacity-building to establish cohesive responses to cybercrime.

31. Moreover, some speakers also expressed appreciation for the release of the Practical Guide for Requesting Electronic Evidence Across Borders. The Guide was jointly drafted and launched by UNODC, the Counter-Terrorism Committee Executive Directorate and the International Association of Prosecutors and was made available to Member States and their criminal justice officials through the UNODC Sharing Electronic Resources and Laws on Crime portal. The Guide, which was produced in collaboration with Member States, international and regional organizations and communication service providers such as Facebook, Google, Microsoft and Uber, contained information on steps that could be taken at the national level to gather, preserve and share electronic evidence with the overall aim of ensuring efficiency in mutual legal assistance practices.

B. Electronic evidence and criminal justice

32. At its 4th and 5th meetings, on 28 and 29 March, the Expert Group considered agenda item 3, entitled “Electronic evidence and criminal justice”.

33. The discussion was facilitated by the following panellists: Mr. Xioafei Zhai (China); Mr. Markko Kunnapu (Estonia); Ms. Camila Bosch (Chile); Mr. Giuseppe Corasaniti (Italy); Mr. Vadim Smekhnov (Russian Federation); and Ms. Briony Daley Whitworth (Australia).

34. During the subsequent debate, the two-fold role of electronic evidence was noted. On the one hand, it was acknowledged that the use of technology and digital infrastructure created more opportunities for perpetrators of serious and organized cyber-dependent and cyber-enabled crime to expand the scope of their illegal activities, target more victims and increase their profits. On the other hand, it was also stressed that electronic evidence was becoming increasingly important in the detection, investigation and prosecution of all types of crime.

35. Many speakers referred to the increasing relevance of electronic evidence in criminal proceedings and described varying national approaches to defining the scope of that evidence. Some speakers noted that there was no commonly agreed definition of electronic evidence at the international level, while the formulation of rules on such

evidence and its admissibility at the national level was the prerogative of Member States. Speakers drew attention to the need for procedural legislation granting powers to competent law enforcement authorities to gather electronic evidence effectively while observing confidentiality, privacy, human rights, due process and other legal safeguards. It was noted that investigative powers could range from traditional procedural powers and general investigative powers to various specific digital investigative techniques.

36. It was agreed that one of the key steps in cybercrime and digital investigations was to preserve the integrity of electronic evidence and ensure its authenticity and admissibility as evidence in related criminal proceedings. In that context, reference was made to national standards, procedures and requirements for handling electronic evidence. The Expert Group again highlighted the necessity of building the capacity and the technical knowledge of competent authorities to deal effectively and efficiently with relevant challenges.

37. The Expert Group considered factors that were relevant when assessing the admissibility of electronic evidence. Emphasis was placed on the importance of compliance with the proportionality principle when using special investigative techniques in cybercrime investigations, including the use of undercover agents and remote forensics, especially on the darknet. It was noted that in many domestic legal systems, that principle was tested primarily by the judicial authority supervising the investigation and by the court, as appropriate. Relevance could be determined on the basis of the seriousness of the offence in question, or the number of persons whose privacy has been violated by the special investigative techniques used; the types of computer data in question; whether a less restrictive alternative measure was available; whether there had been some measure of procedural fairness in the decision-making process; and whether affected persons had adequate opportunities for legal redress.

38. Attention was drawn to the rise of in-built encryption in software and applications, thus rendering access to data as electronic evidence difficult and time-consuming in the absence of the proper decryption keys. Practical suggestions were made on how to overcome that issue, including cooperation with other countries that might have the capacity to access encrypted information, the use of the European Cybercrime Centre and cooperation with the industry, which could develop mechanisms to enable timely access to encrypted data.

39. The use of artificial intelligence in investigations was also mentioned, with particular reference to facial recognition and copyright violations. In general, artificial intelligence might provide solutions enabling the more effective use of time and resources when examining large amounts of data in search of important electronic evidence.

40. Subscriber information was discussed as the type of data most often sought by criminal justice authorities into criminal investigations of cybercrime and other cases involving electronic evidence. In that connection, many speakers referred to challenges regarding subscriber information related to a specific Internet Protocol (IP) address used in a criminal offence. It was noted that, although static IP addresses were stable and assigned to a specific subscriber for the duration of the service arrangement, and although service providers could look up such information in a database of subscribers, service providers might assign an IP address to multiple users. It was therefore necessary to determine the subscriber to whom the IP address had been assigned at a specific moment in time. It was also noted that the reason for the dynamic allocation of IP addresses was that, under Internet Protocol version 4, limited numbers were available. That problem would be resolved once the transition to Internet Protocol version 6 had been completed or was at a more advanced stage.

41. The issue of differentiation between types of requested data and their impact on the effectiveness and timeliness of international cooperation mechanisms to obtain electronic evidence was also discussed. The solutions examined related to, inter alia, strengthening law enforcement cooperation, continuing the multilateral dialogue on

transnational access to computer data and establishing a separate regime for access to subscriber information, as defined in article 18, paragraph 3, of the Budapest Convention.

42. Many speakers referred to the challenges posed by cryptocurrencies in cybercrime investigations. The Expert Group was informed about the UNODC Cryptocurrency Investigation Train-the-Trainers course. The aim of the training was to strengthen the capacity of law enforcement officers, analysts, prosecutors and judges in relation to cryptocurrencies, including how to trace bitcoins in a financial investigation, locate information resources and collaborate on international casework.

43. Under agenda item 3, some speakers discussed jurisdictional issues. Particular reference was made to recent developments in national jurisprudence regarding the interpretation of the territoriality principle in cases where computer data were stored in cloud servers in other jurisdictions.

44. Speakers agreed that international cooperation was of paramount importance for gathering and sharing electronic evidence in the context of cross-border investigations. It was stressed that States should make full use of the Organized Crime Convention and relevant multilateral, regional and bilateral treaties and arrangements on cybercrime to foster international cooperation on judicial assistance and law enforcement in related cases, while respecting the principles of sovereignty, equality and reciprocity. The significance of promoting networking for the sharing of experiences and expertise was highlighted, in particular, to address the challenges posed by varying national requirements on the admissibility and evidentiary integrity and authenticity of such evidence.

45. Priority was accorded by many speakers to the need for sustainable capacity-building within national law enforcement and criminal justice systems, including capacity-building of practitioners from central authorities engaged in international cooperation. It was noted that such capacity-building was essential, particularly for developing countries, both in terms of human resources, infrastructure and equipment, and with a view to bridging the digital divide with developed countries. Overall, it was agreed that building the capacity of law enforcement and criminal justice actors to combat cybercrime would be an ongoing and continuous process, as technological and criminal innovations continued at a rapid pace. Thus, the vast majority of speakers referred to technical assistance and cooperation as important prerequisites for enhancing domestic capabilities and enabling the sharing of good investigative practices and experience and the dissemination of new techniques.

46. In that connection, a number of speakers referred to the challenges posed by limited resources in the field of forensics, a lack of forensic tools and equipment, which were often expensive, and the sheer quantity of data collected for analysis. Challenges in recruiting sufficiently skilled personnel were also reported.

C. Other matters

47. At its 6th meeting, on 29 March 2019, the Expert Group considered agenda item 4, entitled “Other matters”.

48. One speaker requested information about the report on countering the use of information and communications technologies, which was to be submitted to the General Assembly at its seventy-fourth session, pursuant to Assembly resolution 73/187. In response, a representative of the Secretariat referred to the mandate contained in the resolution, stressing that a note verbale had been sent to Member States on 13 February 2019 inviting them to submit information on the challenges that they faced in countering the use of information and communications technologies for criminal purposes and informing them that that information would be used to prepare the report. The deadline for the submission of national feedback was established as Friday, 12 April 2019. After the expiration of that deadline, the

Secretariat would compile the feedback received with a view to finalizing the report in May 2019.

IV. Organization of the meeting

A. Opening of the meeting

49. The meeting was opened by André Rypl (Brazil), Vice-President of the Expert Group, in his role as Chair of the fifth meeting of the Expert Group.

B. Statements

50. Statements were made by experts from the following Member States: Algeria, Argentina, Armenia, Australia, Belarus, Brazil, Burkina Faso, Canada, Chile, China, Colombia, Costa Rica, Dominican Republic, Ecuador, Estonia, France, Georgia, Germany, India, Indonesia, Iran (Islamic Republic of), Italy, Japan, Jordan, Kuwait, Malaysia, Mauritania, Mexico, Morocco, Netherlands, Niger, Nigeria, Norway, Paraguay, Peru, Philippines, Russian Federation, Serbia, Slovakia, South Africa, Spain, Sri Lanka, Thailand, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America and Viet Nam.

51. Statements were also made by representatives of two intergovernmental organizations: Council of Europe and European Union.

C. Adoption of the agenda and other organizational matters

52. At its 1st meeting, on 27 March 2019, the Expert Group adopted the following provisional agenda:

1. Organizational matters:
   (a) Opening of the meeting;
   (b) Adoption of the agenda.
2. Law enforcement and investigations.
3. Electronic evidence and criminal justice.
4. Other matters.
5. Adoption of the report.

D. Attendance

53. The meeting was attended by representatives of 105 Member States, an institute of the United Nations crime prevention and criminal justice programme network, UNODC, intergovernmental organizations and the private sector.

54. A list of participants is contained in document UNODC/CCPCJ/EG.4/2019/INF/1/Rev.1.

E. Documentation

55. The Expert Group had before it, in addition to the draft comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, the following documents:

(a) Annotated provisional agenda (UNODC/CCPCJ/EG.4/2019/1);

(b) Chair's proposal for the workplan of the Expert Group for the period 2018–2021, based on Commission on Crime Prevention and Criminal Justice resolution 26/4 (UNODC/CCPCJ/EG.4/2018/CRP.1).

V. Adoption of the report

56. At its 6th meeting, on 29 March 2019, the Expert Group adopted its report (UNODC/CCPCJ/EG.4/2019/2).