24 August 2020

Original: English

Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 July 2020

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 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 draft 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.

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 on Crime Prevention and Criminal Justice 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 the 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 on Crime Prevention and Criminal Justice 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. The Expert Group also considered the ways in which cybercrime was criminalized at the national level. Also at that meeting, the Expert Group adopted the proposal by the Chair for the workplan of the Expert Group for the period 2018–2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. The fifth meeting of the Expert Group was held in Vienna from 27 to 29 March 2019. At that meeting, the Expert Group focused on law enforcement and investigations and on electronic evidence and criminal justice related to cybercrime. Also at that meeting, the Expert Group discussed, inter alia, successful national efforts to implement legal and procedural measures to tackle cybercrime and measures to implement new investigative tools to gather electronic evidence and establish its authenticity for evidentiary purposes in criminal proceedings. The discussion was 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. The Expert Group accorded priority to the need for sustainable capacity-building for enhancing domestic capabilities and enabling the sharing of good investigative practices and experiences.

9. In its resolution 74/173, the General Assembly acknowledged the importance of the work of 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; noted with appreciation that the Expert Group would develop, in accordance with its workplan for the period 2018–2021, possible conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice; recognized the Expert Group as an important platform for the exchange of information on national legislation, best practices, technical assistance and international cooperation; requested UNODC to continue to periodically collect information on new developments, progress made and best practices identified and to periodically report that information to the Expert Group and the Commission; and invited the Expert Group to provide advice, on the basis of its work, to UNODC, including with regard to the 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, without prejudice to the status of the Commission as the governing body of the crime programme of the Office.

10. The extended Bureau of the Expert Group approved the original dates of 6 to 8 April 2020 for the sixth meeting of the Expert Group by silence procedure on 11 November 2019. The provisional agenda for the sixth meeting was agreed upon by the extended Bureau by silence procedure on 18 December 2019. On 12 March 2020, the extended Bureau was informed that the meeting was to be postponed owing to restrictions related to the coronavirus disease (COVID-19). By silence procedure on 15 April 2020, the extended Bureau approved new dates of 27 to 29 July 2020 for the sixth meeting of the Expert Group. The holding of the sixth meeting in a hybrid/Chair format was approved by silence procedure on 22 June 2020.

II. List of preliminary recommendations and conclusions as compiled by the Rapporteur

11. In line with the workplan of the Expert Group for the period 2019–2021, the Rapporteur, with the necessary assistance of the Secretariat and based on the discussions and deliberations during the meeting, prepared a list of preliminary conclusions and recommendations suggested by Member States, which are precise and are focused on strengthening practical responses to cybercrime. Pursuant to the workplan, the list was included in the report on the sixth meeting as a compilation of suggestions made by Member States, for further discussion at the stocktaking meeting to be held not later than 2021.

12. As provided for in the workplan, at its stocktaking meeting, the Expert Group will consider the accumulated preliminary conclusions and recommendations and will consolidate them in a list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice. Prior to the stocktaking meeting, the preliminary conclusions and recommendations proposed by Member States will be circulated to all Member States, observers and other stakeholders for comments and those comments will be posted online in advance of the stocktaking meeting, for consideration by delegations.

A. International cooperation

13. In line with the workplan of the Expert Group, the present paragraph contains a compilation by the Rapporteur of suggestions made by Member States at the meeting under agenda item 2, entitled “International cooperation”. Those preliminary recommendations and conclusions were made by Member States and their inclusion does not imply their endorsement by the Expert Group, nor are they listed in order of importance:

(a) As regards the scope of the definition of cybercrime for the purposes of international cooperation, countries should ensure the sufficient criminalization of cybercrime acts, which cover not only cyber-dependent crimes, but also other crimes frequently committed with the use of the Internet and electronic means (cyber-enabled crimes), such as cyberfraud, cybertheft, extortion, money-laundering, trafficking in drugs and arms, child pornography[1] and terrorist activities;

[1] The term “child pornography” is firmly anchored in international legal instruments adopted in the twenty-first century. The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography defines the term “child pornography” in its article 2 as “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes”. In addition, through article 3, paragraph (c), of that Optional Protocol, States are required to criminalize the following constituent parts of the offence of child pornography: “producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in article 2.” The Council of Europe Convention on Cybercrime refers, in its article 9, paragraph 2, to the term “child pornography”, which is defined as “pornographic material that visually depicts: (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; and

(b) With regard to international cooperation mechanisms, States were encouraged to accede to and/or use, in the absence of a bilateral mutual legal assistance treaty, existing multilateral treaties such as the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime that provide a legal basis for mutual legal assistance. In the absence of a treaty, States may ask another State for cooperation on the basis of the reciprocity principle; the Council of Europe Convention on Cybercrime should also be used as a standard for capacity-building and technical assistance worldwide, and attention was drawn to the ongoing negotiations on the second additional protocol to it to further enhance cross-border cooperation. The opinion was reiterated that the Council of Europe Convention on Cybercrime was of limited application because of its nature as a regional instrument and its ratification status, as well as its lack of a holistic approach and the fact that it did not take into account current cybercrime trends and was not fully convenient for developing countries. Attention was drawn to General Assembly resolution 74/247, in which the Assembly had decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. A number of delegations expressed the view that the elaboration of a United Nations convention would facilitate the efficiency of international cooperation in the area of fighting cybercrime. Other delegations expressed the view that new frameworks or instruments on cybercrime should not create obstacles or cause States to abandon or go against current treaties or previously assumed commitments, as well as agreements already in place;

(c) It is necessary to have strategic partners, such as the members of existing organizations, including the Organization of American States (OAS), the Group of Seven and the International Criminal Police Organization (INTERPOL), in investigations into cybercrime;

(d) In investigations and judicial proceedings, States' sovereignty and jurisdiction are to be respected. No demands for the direct retrieval of data located in

---

(c) realistic images representing a minor engaged in sexually explicit conduct." Article 20, paragraph 2, of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse contains the term "child pornography", which is defined as "any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes." Under article 20, paragraph 1, of that Convention, parties are to criminalize "producing child pornography, offering or making available child pornography, distributing or transmitting child pornography, procuring child pornography for oneself or for another person, possessing child pornography and knowingly obtaining access, through information and communication technologies, to child pornography." The above have contributed to the use of the term "child pornography" in domestic legislation. Thus, the term remains important for the definition of a crime in many countries. Nevertheless, there is a growing tendency among both law enforcement bodies and child protection agencies to question the appropriateness of the term, and to suggest alternative terminology (see Interagency Working Group on Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (Bangkok, ECPAT International, 2016), pp. 38–40).

Therefore, although the term "child pornography" is still widely used, "child sexual abuse material" has been increasingly used to describe sexually explicit representations of children, as the term is believed to more accurately reflect the grave nature of the content and to challenge any notion that such acts might be carried out pursuant to the consent of the child. The Comprehensive Operational Strategic Planning for the Police Internet Related Child Abusive Material Project, for example, advocates the notion that a sexual image of a child is abuse or exploitation and should never be described as pornography. "Pornography" is a term used for adults engaging in consensual sexual acts distributed legally to the general public for their sexual pleasure. Child abuse images are not. They involve children who cannot and would not consent and who are victims of a crime. Indeed, from a law enforcement perspective, child sexual abuse material is documented evidence of the crime of sexual abuse or rape in progress (UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (New York, 2015), p. 10).

another country should be made to any businesses or individuals without the prior consent of that country;

(e) The efficiency of international cooperation should be improved by establishing rapid response mechanisms for international cooperation, as well as channels of communication through liaison officers and information technology systems between national authorities for the cross-border collection of evidence and online transfer of electronic evidence;

(f) States should continue strengthening cooperation to protect critical infrastructure and strengthen networks of collaboration among computer emergency response teams and computer security incident response teams;

(g) States should consider the creation of innovative protocols for the exchange of information, including intelligence and evidence of criminal acts, in order to expedite such procedures;

(h) There is a need for a renewed confirmation of the commitment of all Member States to ensuring the safety and security of information and communications technology through solely peaceful use and strengthening international efforts to combat any malicious activities in cyberspace in times of major crisis at the global, regional and local levels;

(i) The procedures for international cooperation should be optimized so that maximum assistance is provided within the possibilities derived from domestic legal frameworks for international cooperation requests concerning preservation of electronic evidence and access to log files and user registration information in a way that does not interfere with human rights and fundamental freedoms or property rights;

(j) There is a need to prepare an internationally acceptable standard operating procedure regarding the collection and preservation of data that can be followed at the scene of a crime. Universal adoption of standard international practices on the collection, storage and sharing of evidence are critical, in particular in the process of investigation of cybercrime and prosecution of cybercriminals;

(k) Countries are called upon to pay particular attention to the necessary proportionality of investigative measures, while respecting fundamental freedoms and the personal data protection regimes associated with private correspondence;

(l) International cooperation to combat cybercrime should also take into account gender- and age-sensitive approaches and the needs of vulnerable groups;

(m) States should refrain from taking illegal unilateral measures that are not in accordance with international law and the Charter of the United Nations;

(n) In terms of the scope of international cooperation, while mutual legal assistance should be provided only by national authorities, cooperation should not be limited to government departments, but should also involve the private sector, such as Internet service providers. In that context, it was recommended that provisions needed to be adopted allowing for direct cooperation with Internet service providers in other jurisdictions with regard to requests for subscriber information and preservation requests;

(o) Options to counter cybercrime and to protect societies must always ensure the protection of human rights and constitutional guarantees and promote a more free, open, secure and resilient cyberspace for all;

(p) Countries are encouraged to streamline cooperation with industry and enhance collaboration between the Government and private service providers, in particular for addressing the challenges posed by harmful criminal material on the Internet;

(q) Private companies, notably Internet service providers, have shared responsibility in preventing and investigating cybercrime; such companies should

expedite and expand their responses to legal assistance requests, offer them in the countries in which they are based and ensure that they have appropriate channels for communicating with local authorities;

(r) Public-private partnerships must be strengthened. Where such partnerships do not exist, they must be created and private companies should participate in working groups (multilateral forums) and be a part of the conversation on enhancing the approach to cybercrime;

(s) Non-governmental organizations and academia must also form part of efforts to prevent and counter cybercrime, as they provide an inclusive, multifaceted and comprehensive perspective to, inter alia, ensure the protection of human rights, especially freedom of expression and privacy;

(t) Countries are called upon to join, make wider use of and strengthen authorized networks of practitioners to preserve and exchange admissible electronic evidence, including 24/7 networks, specialized networks on cybercrime and INTERPOL channels for prompt police-to-police cooperation, as well as networking with strategically aligned partners, with a view to sharing data on cybercrime matters and enabling rapid responses and minimizing loss of critical evidence. The use of police-to-police cooperation and other methods of informal cooperation before using mutual legal assistance channels was also recommended;

(u) Each State should set up a genuine 24/7 point of contact, accompanied by appropriate resources, to facilitate the preservation of digital data alongside traditional international mutual assistance in criminal matters, drawing on the successful model of data freezing under the Council of Europe Convention on Cybercrime;

(v) Member States should exchange information on how challenges in accessing digital evidence in a timely manner are being resolved domestically, in order for other Member States to benefit from those experiences and increase the efficiency and effectiveness of their own processes;

(w) Member States should establish practices that allow the transmittal and receipt of mutual legal assistance requests through electronic means to reduce delays in the State-to-State transmission of documents;

(x) Countries should strengthen inter-institutional collaboration and improve interoperability through the standardization of information requests and authentication procedures and multi-stakeholder buy-in;

(y) Countries should improve the implementation of national laws and enhance improved domestic coordination and synergies for the collection and sharing of information and evidence for prosecution purposes;

(z) Member States should establish domestic regimes that make the sharing of “subscriber information”, as defined in article 18, paragraph 3, of the Council of Europe Convention on Cybercrime, faster and more efficient;

(aa) States should strengthen measures for sharing financial or monetary information, freezing accounts and confiscating assets to ensure that criminals cannot enjoy the benefits of criminal activities;

(bb) States are encouraged to establish joint investigative teams with other countries at the bilateral, regional or international levels to enhance enforcement capabilities;

(cc) States should also enable the effective handling of electronic evidence and its admissibility before the court, including where it is destined for, or received from, a foreign jurisdiction. In this regard, countries are encouraged to continue or start reform efforts with regard to legislation on cybercrime and electronic evidence, following positive examples and reforms worldwide;

(dd) The development of legal frameworks that also include aspects of extraterritorial jurisdiction over cybercrime acts is recommended;

(ee) Countries should refine mechanisms to mitigate conflicts and address the challenges of attribution and capacity to investigate cybercrime cases;

(ff) States should work towards standardizing and disseminating procedural tools for the expedited production of data and extending searches (such as production orders and orders for expedited preservation or transborder access) to facilitate the work of law enforcement authorities and their direct cooperation with Internet service providers and solve problems associated with the tracing of electronic evidence and its appropriate use;

(gg) States should facilitate the development and standardization of interoperable technical standards for digital forensics and cross-border electronic evidence retrieval;

(hh) Investment in or the establishment of a strong central authority for international cooperation in criminal matters to ensure the effectiveness of cooperation mechanisms involving cybercrime is recommended. It is also recommended that specific units be established to investigate cybercrime and that preservation requests by another State be addressed through a 24/7 network (or directly with the provider in some circumstances) to preserve the required data as quickly as possible. Increased understanding of the information needed for a successful mutual legal assistance request may assist in obtaining the data more quickly;

(ii) A formal arrangement with organizations such as the European Union Agency for Law Enforcement Cooperation (Europol) European Cybercrime Centre, the Cyber Crimes Center of the United States of America, the Japan Cybercrime Control Center and the National Cyber Security Centre of the United Kingdom of Great Britain and Northern Ireland will be helpful in sharing information related to the latest cybercrime threats, modi operandi, emerging technology for cybercrime investigations and access to each other, best practices, etc.;

(jj) Effective international cooperation requires national laws that create procedures that enable international cooperation. Thus, national laws must permit international cooperation among law enforcement agencies;

(kk) States should carry out effective extradition cooperation. If a requested State intends to refuse to extradite a cybercriminal suspect, it should, upon request, make every effort to consult with the requesting State, so as to give the requesting State the opportunity to express its opinion and provide information. A requested State should provide the grounds of refusal to the requesting State;

(ll) Beyond domestic laws, international cooperation on cybercrime relies on both formal, treaty-based cooperation and traditional police-to-police assistance. When debating a new instrument on cybercrime, it is important that countries remember that a new instrument should not conflict with existing instruments, which already enable real-time international cooperation for many. Thus, countries should ensure that any new instrument on cybercrime avoids conflict with existing treaties;

(mm) Sustainable capacity-building and technical assistance to increase capabilities across operational areas and strengthen the capacity of national authorities to respond to cybercrime should be prioritized and increased, including through networking, joint meetings and training, the sharing of best practices, training materials, and templates for cooperation. Such capacity-building and training should include highly specialized training for practitioners that promotes, in particular, the participation of female experts, and should address the needs of legislators and policymakers to better handle issues of data retention for law enforcement purposes. The capacity-building and training should also be focused on improving the abilities of law enforcement authorities, investigators and analysts in forensics, in the use of open source data for investigations and in the chain of custody for electronic evidence,

as well as in collecting and sharing electronic evidence abroad. Another focus of the capacity-building and training should be on improving the abilities of judges, prosecutors, central authorities and lawyers to effectively adjudicate and deal with relevant cases;

(nn) It is imperative to develop adequate and, if possible, uniform data-retention and data-preservation rules and timelines to ensure that electronic evidence can be preserved or obtained to support further mutual legal assistance requests;

(oo) International cooperation is important for gathering and sharing electronic evidence in the context of cross-border investigations and for fast and effective responses to requests for mutual legal assistance related to preserving and obtaining electronic evidence. The principles of sovereignty and reciprocity should be respected in the process;

(pp) UNODC is encouraged to further provide capacity-building and training programmes in combating cybercrime to national governmental experts to strengthen capacities to detect and investigate cybercrime. Such capacity-building should 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 practitioners and stakeholders;

(qq) UNODC has developed the Mutual Legal Assistance Request Writer Tool to assist criminal justice practitioners in drafting mutual legal assistance requests. The Office has also developed the *Practical Guide for Requesting Electronic Evidence Across Borders*, available on request to government practitioners in Member States. Countries may benefit from employing those key tools developed by UNODC;

(rr) The Commission on Crime Prevention and Criminal Justice should consider extending the workplan of the Expert Group beyond 2021 as a forum for practitioners to exchange information on cybercrime;

(ss) It was recommended by some speakers that the negotiation and adoption of a United Nations convention to promote cooperation in combating cybercrime would facilitate improving the efficiency of international cooperation in the fight against cybercrime;

(tt) It was recommended that any elaboration of a new convention should be handled among the experts in UNODC in Vienna;

(uu) Some speakers recommended that the Commission on Crime Prevention and Criminal Justice should renew the mandate of the Expert Group and decide upon a workplan beyond 2021, which should also include emerging forms of cybercrime and the examination of issues related to online sexual abuse and exploitation of children;

(vv) Further, it was recommended that the open-ended ad hoc intergovernmental committee of experts established pursuant to General Assembly resolution 74/247 to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes should start its work only after the Expert Group had agreed upon its recommendations and sent them to the Commission on Crime Prevention and Criminal Justice, in 2021;

(ww) However, other speakers stated that there was no need for the continuation of the work of the Expert Group beyond 2021, in view of the adoption of General Assembly resolution 74/247. That would enable a focus on the implementation of that resolution and the negotiation of a new convention, and would make best use of the resources available;

(xx) In their statements, the representatives of many Member States welcomed the adoption of General Assembly resolution 74/247. It was stated that the elaboration of the new convention pursuant to that resolution should be inclusive, transparent and based on consensus, for which the earlier United Nations processes to conclude the

Organized Crime Convention and the United Nations Convention against Corruption could be considered examples;

(yy) There were calls for the active participation of all Member States in the work of the ad hoc committee to develop a new convention;

(zz) At the same time, other speakers stated that, in terms of content, any new convention should take into account, and not be in conflict with, existing frameworks and instruments. It was recommended that the issues of cross-border collection of evidence, criminalization provisions and respect for sovereignty be included in a possible new convention;

(aaa) The international community should prioritize the provision of capacity-building and other support to strengthen the ability of national authorities to respond to cybercrime and, in particular, to child sexual abuse and exploitation online;

(bbb) Member States should afford each other mutual legal assistance to the widest extent possible to obtain electronic evidence, including in cases involving the use of information and communications technologies to commit or incite terrorism or the financing of terrorism; it was further stated that private sector entities had a responsibility to cooperate with national authorities in that regard;

(ccc) Member States should consider investing in specialized centralized cybercrime forces and in regional technological units for criminal investigations;

(ddd) Member States should also consider establishing separate cybercrime units within central authorities for mutual legal assistance as a base of expertise in the complex area of international cooperation. Such specialized units not only provide benefit in the day-to-day practice of mutual legal assistance, but also allow for focused capacity-building assistance such as training to address the needs of domestic and foreign authorities on how to obtain mutual legal assistance involving electronic evidence quickly and efficiently in cyber-related matters;

(eee) Member States should consider maintaining electronic databases that facilitate access to statistics relating to incoming and outgoing requests for mutual legal assistance involving electronic evidence, to ensure that reviews of efficiency and effectiveness are in place;

(fff) Member States should be reminded to utilize central authorities in transmitting requests for mutual legal assistance and in working with competent authorities for the execution of such requests to ensure compliance with existing treaties and to reduce delays in the process;

(ggg) For acquiring data to conduct investigations in relation to cybercrime acts, States should build on tried-and-tested international instruments, as such investigations are complex and require an institutional framework that has proved its resilience and added value. The Council of Europe Convention on Cybercrime, which has provided the standard for acquiring electronic evidence over the years, yielding results on a daily basis for law enforcement agencies around the world, was highlighted in that respect. It was recommended that States reduce conflicts of law regarding applicable legal requirements by taking into account, in the case of direct production orders, the legislation of the State in which the requested Internet service provider is located or the legislation of the State of which the suspect is a national as a starting point;

(hhh) The creation of a framework is recommended where it is clear that, in case of “loss of location”, the decision to proceed with an investigation requires an effort to establish which territory is affected and where the integrity of automated networks is vital in order to be able to consult on matters of jurisdiction and the most appropriate way to continue the investigations;

(iii) It was recommended that international law, including the principles of sovereignty, territorial integrity and non-intervention in domestic affairs, should be applicable in cyberspace, that information and communications technologies should

not be employed as weapons and that State-sponsored attacks must be condemned and those responsible should be held accountable;

(jjj) Subject to its domestic law, a requested State should provide maximum assistance to investigation and evidence collection requests that do not involve personal freedom or property rights, or that have a de minimis impact on such rights;

(kkk) States should establish a quick-response mechanism and communication channel for judicial assistance and law enforcement cooperation in combating cybercrime, and consider enabling the online exchange of legal documents and electronic evidence, supported by electronic signatures and other technical means;

(lll) The international community should formulate a unified procedure for cybercrime investigation techniques and improve regulations on the log preservation obligations of Internet service providers in their domestic laws;

(mmm) States should prevent international transfers of illicit proceeds obtained from cybercrime and strengthen international cooperation in asset recovery relating to cybercrime;

(nnn) States should respect the sovereignty of other States when establishing their jurisdiction over cybercrime and should not exercise excessive extraterritorial jurisdiction that lacks a sufficient and genuine link with the prosecuted cybercrime. States are encouraged to enhance communication and consultation to settle jurisdictional conflicts;

(ooo) It is important to ensure the safe and secure use of information and communications technologies in providing connectivity and awareness for everyone across the globe, regardless of the status of the territories in which the users reside.

B. Prevention

14. In line with the workplan of the Expert Group, the present paragraph contains a compilation by the Rapporteur of suggestions made by Member States at the meeting under agenda item 3, entitled “Prevention”. The preliminary recommendations and conclusions were made by Member States and their inclusion does not imply their endorsement by the Expert Group, nor are they listed in order of importance:

(a) It should be recognized that prevention is not just the responsibility of Governments: it also requires the participation of all relevant stakeholders, including law enforcement authorities, the private sector, especially Internet service providers, non-governmental organizations, schools and academia, in addition to the public in general;

(b) It was recommended that the public should have easy access to prevention tools such as online platforms, audio clips, plain-language infographics and reporting platforms;

(c) It was deemed necessary to develop a series of long-term public policies on prevention, which should include the development of awareness-raising campaigns on the safe use of the Internet;

(d) Cybersecurity awareness should be included as a subject in primary, secondary and tertiary education, for both students and teachers. This should ideally be part of a national cybersecurity strategy. States should also share experiences on how to use cybersecurity strategies to prevent cybercrime. In addition, States should devote special attention to preventive measures addressed at youth, including first-time offenders, in order to prevent reoffending;

(e) When preventing and combating cybercrime, States should pay special attention to the issues of preventing and eradicating gender-based violence, in particular, violence against women and girls, and hate crimes;

(f) Preventive activities must be proactive, regular, continuous and suitable for vulnerable groups;

(g) The intersection of and collaboration between the public and private sectors with regard to big data sets or big data centres can present an area of high vulnerability, in particular, but not only, in the health sector, as seen during the current pandemic. States should devote specific attention to regulating the legal access to such data and protecting them from cyberattacks;

(h) With regard to preventive efforts, Internet service providers should undertake more responsibility for security precautions ("by default") and the prevention of cybercrime, and international standards should be developed on the content and duration of log information to be retained by the Internet service providers. Moreover, the responsibilities of Internet service providers to detect, prevent and disrupt cybercrime should be clearly defined;

(i) Public-private partnerships, including cooperation with cybersecurity stakeholders and big technology companies on information-sharing, are needed to prevent and combat cybercrime;

(j) States should provide training for specialized magistrates and judges who handle cybercrime cases and provide investigative bodies with high-performance tools for tracing cryptocurrencies and addressing their use for criminal purposes;

(k) States should step up strategies to combat the use by traditional criminal groups of cybertools to hide their communications and activities;

(l) Solutions should be developed for direct cooperation between national authorities and Internet service providers, while upholding the rule of law and human rights, including data protection requirements;

(m) States should ensure the freedom of the press when developing measures to prevent cybercrime;

(n) It was recommended that the collective capabilities of competent institutions be built and the prevention culture changed from reactive to proactive. It was also recommended that a robust mechanism to stimulate and facilitate the sharing of intelligence on potential criminal modi operandi be put in place;

(o) Member States are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities such as raising awareness about the risks of cybercrime, targeting such campaigns at modi operandi such as phishing or malware ("ransomware") and at different groups such as youth and elderly people. Member States are also encouraged to continue to focus on the likelihood of prosecution and punishment of offenders and efforts to prevent crime by identifying and disrupting ongoing illicit activities online. Police and public prosecution services should invest in signalling, detecting and reacting to cybercrime threats. Public-private partnership is indispensable. These prevention activities do not require extra laws or regulations;

(p) Owing to the existence of the "digital gap", some developing countries lack the capacity to prevent, detect and combat cybercrime and are more vulnerable in the face of cybercrime challenges;

(q) UNODC was strongly encouraged to continue providing technical assistance, upon request, to prevent and counter cybercrime;

(r) Future international tools on the prevention of cybercrime should be accessible to everyone across the world, without any distinction on the basis of the status of the country or territory of which a person is a national or a resident;

(s) Basic human rights and fundamental freedoms should be protected everywhere, including in the digital domain and cyberspace, regardless of frontiers and without any interference or limitation;

(t) Cyberspace and cybercrime are not territorially bound and do not recognize any borders or other physical restrictions. Therefore, the international community should remain united in curbing cyberthreats;

(u) Cyberspace is a unique and global area and, in the absence of an international code of conduct, further efforts should be taken to develop rules, principles and norms of responsible State behaviour in cyberspace. In this context, all Member States should renounce the threat or use of force against the critical infrastructure of other States;

(v) Member States are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities, such as raising awareness about the risks of cybercrime and the likelihood of prosecution and punishment for offenders and efforts to prevent further crime, by identifying and disrupting ongoing illicit online activities;

(w) Cybersecurity practices are distinct from efforts to combat cybercrime. States should develop both a national cybercrime strategy, including national legislation or policy for cybercrime prevention, and a national cybersecurity strategy. Focus areas for national cybercrime strategies should include cybercrime prevention, public-private partnerships, criminal justice capacity and awareness-raising through published court decisions;

(x) Countries should collect a broad range of data to help understand trends to inform and shape cybercrime policies and operational responses to combat cybercrime;

(y) Efforts in the development of strategies for cybercrime prevention should also take into account the protection of human rights;

(z) "Criminal justice capacity" should be another area of focus in national cybercrime strategies. Assistance to developing countries should be a priority in order to strengthen law enforcement capacity in preventing cybercrime;

(aa) Member States should avail themselves of capacity-building assistance from the UNODC Global Programme on Cybercrime and other initiatives, including the Council of Europe Global Action on Cybercrime Extended programmes;

(bb) States should develop or strengthen support programmes for victims of cybercrime;

(cc) States should undertake surveys to measure the impact of cybercrime on businesses, including measures implemented, employee training, types of cyberincidents that affect them and the costs associated with recovering from and preventing cyberincidents;

(dd) States should support businesses and communities in raising awareness of cybercrime risks, mitigation strategies and enhancing cyberpractices, as these can have significant downstream preventive benefits;

(ee) The modi operandi of contemporary cybercriminals should be carefully studied by means of intelligence analysis and criminological research in order to deploy existing resources more effectively and identify vulnerabilities;

(ff) States should consider setting up a coordination platform to promote the instant exchange of data on incidents and new trends in cybercrime that have been identified. States should also consider establishing criminological observatories to monitor cybercrime threats and trends;

(gg) Countries should consider specific and tailored efforts to keep children safe online. This should include ensuring domestic legal frameworks, practical arrangements and international cooperation arrangements to enable reporting, detection, investigation, prosecution and deterrence of child sexual abuse and exploitation online;

(hh) Industry is a key partner in preventing cybercrime. Countries should consider implementing mechanisms for cooperating with industry, including on referrals to competent national authorities and takedowns of harmful criminal material, including child sexual exploitation and abhorrent violent material;

(ii) Regular advisories on incident prevention should be issued and shared with users, organizations and other stakeholders to enable them to prevent cyberincidents that could potentially lead to criminal activities;

(jj) There should be a methodology and standard procedures for sharing live information based on evidence to prevent cybercrime;

(kk) A mechanism should be developed to register all online services and to implement minimum baseline security standards through domestic regulation;

(ll) States should consider using artificial intelligence to design systems that automatically reconfigure themselves in the face of attacks;

(mm) It was recommended that a global database on cryptocurrency abuses and the exploitation of data by criminals on a large scale should be created, as well as a globally coordinated strategic overview of the threats posed by criminal offences committed on the darknet;

(nn) Regional and international initiatives aimed at strengthening cybersecurity should be encouraged, in particular the exchange of information on large-scale cyberattacks;

(oo) States may consider establishing an international cyberthreat information-sharing system to share and study the technologies and modi operandi of new threats;

(pp) States are encouraged to establish a tiered cybersecurity protection system to adopt different information security technologies and management measures for different information and communications facilities and to ensure that critical infrastructure is protected from cybercrime;

(qq) States should involve female experts in the prevention and investigation of cybercrime;

(rr) National and regional prevention experiences should be brought together to create a multilateral repository that would allow the dissemination of good practices in diverse contexts;

(ss) Measures should be strengthened with the aim of preventing the spread of hate speech, extremism and racism;

(tt) Greater awareness should be generated and legislative assistance should be provided on regulatory frameworks against cyberbullying and online threats of violence or abuse;

(uu) Capacity-building and cooperation should be provided for the prevention of cybercrime with other regional actors and organizations (such as OAS) and with multi-stakeholder forums such as the Global Forum on Cyber Expertise;

(vv) States are encouraged to take the opportunity to negotiate a new convention on combating cybercrime to formulate uniform standards in the field of prevention in order to coordinate the actions of various countries more effectively;

(ww) It was recommended that States invest in capacity-building to upgrade the skills of officers from the whole spectrum of the criminal justice system as an efficient preventive measure of deterrent effect against cybercrime;

(xx) UNODC should facilitate the sharing of best practices on effective and successful preventive measures against cybercrime.

III. Summary of deliberations (summary by the Chair)

15. The following summary of deliberations stemming from the meeting was prepared by the Secretariat after the meeting, in close coordination with the Chair, pursuant to the proposed organization of work for the meeting, which had been circulated to the extended Bureau of the Expert Group on 13 July 2020 and was approved by the Group at the opening of the meeting. The summary of deliberations was not discussed and, consequently, was not subject to adoption during the meeting. It was, instead, a summary by the Chair, as set out in sections A-C below.

A. International cooperation

16. At its 1st, 2nd and 3rd meetings, on 27 and 28 July 2020, the Expert Group considered agenda item 2, entitled “International cooperation”.

17. The discussion was facilitated by the following panellists: George-Maria Tyendezwa (Nigeria), Gangqiang Zhang (China), Amornchai Leelakajonjit (Thailand), Markko Künnapu (Estonia), Vadim Sushik (Russian Federation), Pedro Janices (Argentina), Stephen McGlynn (Australia) and Sheri L. Shepherd-Pratt (United States).

18. During the discussion, speakers referred to the rapid increase in cybercrime, also in the light of the challenges posed by the COVID-19 pandemic, and stressed the significance of enhancing international cooperation to address effectively the scourge of cyber-dependent and cyber-enabled crimes, which were of a transnational nature and involved high standards of criminal sophistication and adaptation to changing circumstances and priorities. In that regard, many speakers made reference to national action and/or reforms to develop and implement cybersecurity strategies and policies; enact and/or upgrade legislation on cybercrime; implement new investigative tools to gather electronic evidence; and, on the basis of robust domestic measures and improved capabilities and infrastructure, promote international cooperation to combat cybercrime.

19. Speakers noted that the challenges posed by the lack of harmonization of criminalization provisions, the lacunae in procedural powers for law enforcement and criminal justice authorities and the conflicts of jurisdiction when securing electronic evidence called for the renewal of the commitment of Member States to achieving effective and strengthened regional and international cooperation to combat cybercrime. In that regard, it was highlighted that, while international cooperation played a vital role in tackling and preventing cybercrime, it should be promoted in conjunction with the principles of sovereignty, respect for national laws and, in the absence of an applicable treaty, reciprocity, also taking into account the different levels of capacity and resources of Member States, especially developing countries.

20. It was noted that, since the previous meeting of the Expert Group, there had been developments in the Third Committee of the General Assembly that had added another dimension to the international cybercrime conversation, namely the adoption by the Assembly of resolution 74/247, in which the Assembly had decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

21. A number of speakers expressed the view that the elaboration of a convention to combat cybercrime within the framework of the United Nations would facilitate the efficiency of international cooperation in the area of fighting cybercrime and would be the most appropriate response to cybercrime at the international level. In that connection, they underscored that a new global instrument against cybercrime would take into account, inter alia, the concerns and interests of all Member States, particularly developing countries, and would contribute to filling legal gaps in that area. Some of those speakers were of the opinion that the Council of Europe

Convention on Cybercrime was of limited application because of its nature as a regional instrument and its ratification status, and because it lacked a holistic approach, given that it did not take into account current cybercrime trends and was not fully convenient for developing countries.

22. Other speakers, however, were in favour of making the best use of existing international instruments or frameworks and mechanisms such as the Organized Crime Convention, the Council of Europe Convention on Cybercrime and INTERPOL. Regarding the Organized Crime Convention, in particular, some speakers stressed that it could be a very useful instrument for international cooperation to combat cybercrime. One speaker confirmed that her country had sent and received numerous requests for assistance relying on the provisions of that Convention as a legal basis for international cooperation involving electronic evidence in cybercrime cases. In further support of the use of that instrument, the same speaker noted that, in the majority of significant cases, cybercrime originated in some form of organized crime, such as activities in underground "markets," with criminal perpetrators in more than one country, and that cybercrime cases involving an organized criminal group often substantially outnumbered the instances in which individual hackers were the main criminal actors.

23. A number of speakers were of the view that the Council of Europe Convention on Cybercrime provided an adequate framework for developing appropriate domestic and international responses to cybercrime. Those speakers recalled that, with 65 States parties, of which 21 were non-States members of the Council of Europe, the Convention was used as a basis for efficient international cooperation, a model for developing national legislation and a standard for capacity-building and technical assistance. In their view, that Convention would remain the most relevant and forward-leaning multilateral agreement on cybercrime for the foreseeable future, being available to countries seeking an immediate path to legislative reforms on cybercrime, stronger law enforcement capacity and increased international cooperation, all without prejudice to future discussions on a new instrument within the framework of the United Nations. However, one speaker also noted that the Convention also faced challenges of weak implementation in certain jurisdictions and, therefore, building responses on the basis of its provisions should be considered as a process of constant evolution.

24. Reference was made to the ongoing negotiation process for the adoption of a second additional protocol to the Council of Europe Convention on Cybercrime, aimed at providing clear rules and more effective procedures in relation to 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.

25. Some speakers drew the attention of the Expert Group to the experiences in international cooperation that had arisen in the field of regional organizations, such as OAS, and regional networks, such as the Police Community of the Americas, while one speaker mentioned that his country continued to work closely with the African Police Cooperation Organization (AFRIPOL) to combat cybercrime.

26. Bearing in mind the ongoing discussions on reaching agreement on the outline and modalities for the further activities of the ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, it was stressed that the new convention should be aimed at an inclusive approach and the highest possible number of ratifications and/or accessions, following the successful examples of the Organized Crime Convention and the Convention against Corruption. There was also a call for a transparent, inclusive and consensus-based treaty-making process, informed by the findings and recommendations of the Expert Group, and taking into account the progress that the international community had already made,

as well as the need for the promotion of a free, open and secure Internet and the protection of human rights online, including the protection of personal data and the right to privacy. Some speakers noted that any new convention should be elaborated on a consensual basis and take into account, and not be in conflict with or duplicate, existing frameworks and instruments; it should not create obstacles or cause States to abandon or go against previously assumed commitments.

27. Some speakers noted that, with the advancement of cloud technology, an increasing amount of electronic evidence was stored on servers outside the territorial jurisdiction of Member States. Given the transnational and volatile nature of such electronic evidence, direct cooperation focusing primarily on intelligence-sharing was mentioned as a very useful tool to address the time constraints and challenges posed by urgent circumstances through shortening the period needed for activating mutual legal assistance channels. It was noted that direct cooperation still relied on mutual trust, but would also benefit from the standardization of requests and expedited data preservation, as well as the more frequent use of mechanisms already in place, such as the I-24/7 global police secure communications system established by INTERPOL, as well as computer security incident response team networks, both private and public. Moreover, the creation of innovative protocols for the exchange of information and evidence might be needed for expediting such procedures.

28. It was noted that one of the key steps in cross-border cybercrime and digital investigations was preserving the integrity of electronic evidence and ensuring its authenticity and admissibility as evidence in related criminal proceedings, with issues such as chain of custody and forensic copies being essential. From that perspective, it was noted that priority should be accorded to the improvement of special investigative techniques, not only for gathering electronic evidence, including on the darknet, but also for conducting financial investigations. In that regard, one speaker stated that measures to counter money-laundering and the financing of terrorism, as well as asset recovery measures, needed to be a strong part of the law enforcement response to cybercrime. Other speakers referred to the challenges posed by cryptocurrencies in investigating and prosecuting illicit flows relating to the proceeds of crime. A number of speakers highlighted the necessity and significance of exploring ways and means to enable criminal justice and law enforcement practitioners to utilize and take full advantage of evolving technologies, such as artificial intelligence, and information and communication technologies, including big data, in the fight against cybercrime.

29. In the field of mutual legal assistance, the expeditious execution of mutual legal assistance requests was identified as one of the most important conditions for effective measures against cybercrime and other offences involving electronic evidence. Some speakers referred to factors that had a negative impact on the efficiency of mutual legal assistance in the field of cybercrime, including different legal requirements and criminalization approaches that hampered the fulfilment of the double criminality requirement, as well as the lack of standardized content and format of relevant requests.

30. In order to expedite international cooperation and streamline mutual legal assistance processes, it was suggested that a separate regime be put in place for access to subscriber information. In that connection, it was noted that, in the ongoing discussions on the second additional protocol to the Council of Europe Convention on Cybercrime, measures were being considered to obtain subscriber information in a more expeditious manner.

31. One speaker referred to key measures that countries could take to reduce the length of time required for the execution of mutual legal assistance requests, including capacity-building and training on country-specific requirements for mutual legal assistance requests to reduce response times and facilitate the execution of a request without extended additional communications for obtaining additional information; and the use of direct channels of communication between central authorities instead of formal, diplomatic channels.

32. Some speakers stressed the need to modernize, streamline and expedite mutual legal assistance practice through the electronic transmission of international cooperation requests, a practice that had recently been followed by some Ibero-American countries. In that connection, it was suggested that central and other competent authorities transmit, through electronic mail, requests for assistance, both formal and inter-institutional, as well as preservation requests, using 24/7 networks.

33. Some speakers referred to transborder access to stored computer data, recalling that the Council of Europe Convention on Cybercrime contained a specific provision (article 32) on it and emphasizing that related measures should be carefully implemented to balance the need for investigations with the protection of human rights and the sovereignty of States.

34. Many speakers placed emphasis on the significance of networking for enhancing international cooperation to address cybercrime. It was noted that 24/7 networks, with responsible contact points in each participating country, played a vital role in facilitating cooperation, particularly with regard to emergency situations. Such networks also facilitated requests for the preservation of data that often became the subject of a request for mutual legal assistance at a subsequent stage; such preservation requests were routinely handled in days, if not hours. It was widely acknowledged that the risk of delays in cybercrime investigations – as evidence could be deleted quickly and data could be lost or modified – made membership in a 24/7 network or contacts with liaison officers essential. For that reason, speakers agreed that central and other competent authorities should build relationships and further strengthen mutual trust through direct communication and consultations, and also through regional and international judicial and law enforcement networks or specialized networks against cybercrime. Examples mentioned in that regard included the recently established judicial cooperation network in South-East Asia (SeaJUST network); Cybernet (a network of the Ibero-American Association of Public Prosecutors (AIAMP), bringing together the specialized contact points from the public prosecutors and ministries of all AIAMP member States); and the Criminal Cooperation Network of AIAMP.

35. Some speakers were of the view that specialized cybercrime structures or units within central authorities could serve as a base of expertise in the complex area of international cooperation. Such specialized structures or units could offer necessary resources and experience in the day-to-day operation of the mutual legal assistance regime and also allow for focused training to be provided to domestic and foreign authorities on how to obtain assistance and electronic evidence in a timely and efficient manner in cyber-related cases.

36. Many speakers highlighted 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 and facilitate timely responses to cybercrime, especially in transnational cases. It was suggested that a frame of reference or guide be created to facilitate a common understanding of requirements and processes by both sides. It was stressed that provisions needed to be in place allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information and requests for the preservation of data. The hope was expressed that the second additional protocol to the Council of Europe Convention on Cybercrime, which was under negotiation, would offer a more complete solution for direct cooperation with private sector entities.

37. One speaker underscored that INTERPOL played a unique role in facilitating police-to-police cooperation, through the national central bureaux in each country, the I-24/7 system and its notices and databases; and that the INTERPOL Global Cybercrime Programme, in particular, had developed cyber analytical platform and collaboration capabilities for knowledge exchange and operational coordination.

38. Priority was accorded by many speakers to the need for sustainable capacity-building within national law enforcement and criminal justice systems, including the

capacity-building of practitioners from central authorities engaged in international cooperation. It was noted that such capacity-building was essential, particularly for developing countries, in terms of human resources, infrastructure and equipment, and bridging the digital divide with developed countries.

39. There was broad agreement that capacity-building and technical assistance based on existing instruments were valuable and effective tools in the fight against cybercrime, and should therefore be further developed and prioritized, while respecting the priorities of Member States. In that regard, a number of speakers expressed their support, either as donors or recipients of assistance, for the UNODC Global Programme on Cybercrime and other technical assistance programmes or frameworks, such as that of INTERPOL, the Global Action on Cybercrime Extended programmes of the Council of Europe and the cybersecurity programme in the context of the Boe Declaration on Regional Security of the Pacific Islands Forum.

40. In relation to the role of UNODC, many speakers focused on encouraging the Office to further provide capacity-building and training programmes on combating cybercrime to competent experts, with a view to strengthening national capacities to detect and investigate cybercrime and to facilitate the sharing of best practices on effective and successful preventive measures against cybercrime. In particular, the need was stressed for the training of different actors in the criminal justice and law enforcement fields, including judges, prosecutors and security agents; the creation and adequate structure of specialized units for the investigation and prosecution of cybercrime acts; and ensuring access to cutting-edge technologies for cybercrime investigations and digital forensics. Some speakers stated that relevant capacity-building initiatives should 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 practitioners and stakeholders.

41. One speaker referred to the importance of the training of law enforcement officers and the work done by the cybercrime academy of the European Union Agency for Law Enforcement Training and the International Law Enforcement Academy. The importance of international cooperation in the field of training and education was also emphasized. Some speakers expressed support for the provision of training to specialized magistrates and judges handling cybercrime cases and the provision of high-performance tools to investigative bodies for tracing cryptocurrencies and addressing their use for criminal purposes.

42. Some speakers highlighted innovations such as the inclusion of an electronic evidence module in the redeveloped UNODC Mutual Legal Assistance Request Writer Tool that might assist in streamlining mutual legal assistance processes involving electronic evidence. Similarly, reference was made to the *Practical Guide for Requesting Electronic Evidence Across Borders* as part of the role of UNODC to provide technical assistance to Member States.

43. A number of speakers stressed that Member States should refrain from taking illegal unilateral measures that were not in accordance with international law and the Charter of the United Nations and that prevented the full economic and social development of the populations of affected countries. It was stated that such unilateral coercive measures had impaired cooperation with national law enforcement authorities in the investigation and prosecution of crimes committed through the use of information and communications technologies, as well as in the transfer of the technological tools necessary for preserving electronic evidence and conducting digital forensic examinations.

44. Some speakers expressed their concern about cyberattacks against critical infrastructure sectors, including the health sector, launched by some Member States or State-sponsored groups and stressed that such action should be strongly condemned and that the persons involved should be held accountable. Another speaker expressed great concern about the fact that the COVID-19 pandemic had created a new reality for the health sector, which had become a direct target and collateral victim of

cybersecurity attacks, in addition to the overwhelming health-care challenges encountered.

45. Some speakers were of the view that the Commission on Crime Prevention and Criminal Justice should consider extending the workplan of the Expert Group beyond 2021 in order to retain a forum for experts and practitioners to exchange information on cybercrime, including for the purpose of examining approaches to child sexual abuse and exploitation online and other emerging forms of cybercrime. Other speakers underlined that, upon completion of the workplan of the Expert Group at its stocktaking meeting in 2021, there was no reason to extend its mandate, in the light of General Assembly resolution 74/247 and the need to focus on the implementation of that resolution, the negotiation of the new convention and making the best use of available resources.

46. One speaker noted that, although the mandates of the Expert Group and General Assembly resolution 74/247 were different, attention should be focused on convergence and complementarities. In view of that, international cooperation and capacity-building, which had been advanced by the Expert Group, should be reflected as pillars of the future work of the ad hoc committee in charge of negotiating the new convention.

47. Another speaker underscored that the ad hoc committee should start its work only after the Expert Group had concluded its recommendations and sent them to the Commission on Crime Prevention and Criminal Justice, in 2021.

B. Prevention

48. At its 4th and 5th meetings, on 28 and 29 July 2020, the Expert Group considered agenda item 3, entitled “Prevention”.

49. The discussion was facilitated by the following panellists: Destino Pedro (Angola), Liyun Han (China), Benjaporn Watcharavutthichai (Thailand), Horacio Azzolin (Argentina), Claudio Peguero (Dominican Republic) and Pedro Verdelho (Portugal).

50. During the discussion, it was noted that cybercrime prevention had become an important component of national policies and strategies to prevent and counter cyberattacks and threats and diminish the vulnerabilities of cyberinfrastructure and obtain effective management of all related risks. The prevention of cybercrime was considered within the framework of a comprehensive approach to fighting cybercrime that could be implemented on a large scale to make the Internet and related communications technologies always available and safer for users and also enhance cooperation in all sectors and at all levels between the actors involved at the national and international levels.

51. A number of speakers highlighted that, as Member States developed wide-ranging strategies for cybercrime prevention, they should be mindful of their international human rights obligations. A view echoed by other speakers was that the formulation of strategies and proposals related to the prevention of cybercrime should be based on a comprehensive vision that considered the possible differentiating and asymmetric impacts on different population groups within a country, but also on different countries, especially in view of the digital gap between developed and developing countries and the fact that some developing countries lacked the capacity to prevent, detect and combat cybercrime and were more vulnerable to cybercrime challenges.

52. It was noted that, in certain jurisdictions, collaboration on cybersecurity was distinct from programmes to support cybercrime investigations and that, although often seen as two sides of the same coin, enforcement policies against cybercrime were uniquely a government responsibility, whereas cybersecurity was the responsibility of a range of public and private actors. Furthermore, it was reported that public and private organizations continued to promote awareness-raising among

businesses with programmes intended to improve the cybersecurity skills of business information technology staff.

53. Multi-stakeholder cybercrime strategies were identified by many speakers as a vital preventive element in the fight against cybercrime. It was underscored that the legal, technical and institutional challenges posed by cybercrime were far-reaching and could be addressed only through coherent and inclusive strategies based on existing initiatives and the role of different stakeholders. From that perspective, the necessity of promoting and increasing the participation of all relevant actors in the prevention of cybercrime was stressed and it was noted that regional organizations, the private sector and academia could provide key support, particularly to developing countries, to achieve a global culture of cybersecurity.

54. Many speakers echoed the need for public institutions such as law enforcement and criminal justice authorities and communication service providers to create public-private partnerships based on mutual trust and confidence in response to the multifaceted challenges encountered in the fight against cybercrime. The importance of having good public-private partnerships was emphasized, in particular with regard to detecting and reporting crimes, providing information on the location of suspects and victims, and providing other data as necessary. From the perspective of partnerships, reference was also made to the need for service providers to undertake more responsibilities for security precautions as preventive measures against cybercrime. Such responsibilities should be clearly defined. It was also underlined that any solutions to be developed for the direct cooperation of national authorities with Internet service providers should be based on the rule of law and human rights, including data protection requirements.

55. Some speakers drew the attention of the Expert Group to the responsibility not only of States but also of companies and other actors in the protection of data that enabled respect for the right to privacy, an issue considered to be central in the area of prevention of cybercrime, similarly to the rights to freedom of expression and of the press. Industry was mentioned as a key partner in preventing cybercrime that could work with public authorities on such issues as referrals to competent national authorities and takedowns of harmful criminal material, including child sexual abuse and abhorrent violent material.

56. The role of non-governmental organizations and academia was highlighted in the context of inclusive and comprehensive strategies on the prevention and investigation of cybercrime that took into account protection of human rights, especially freedom of expression and privacy.

57. Many speakers were in favour of effective prevention measures at both the national and international levels that would include the prosecution and punishment of offenders and efforts to prevent further crime by identifying and disrupting ongoing illicit online activities. That aspect was considered a significant component of preventive policies because of its deterrent effect and was discussed in conjunction with the necessity of investing in capacity-building to upgrade the skills of officers from the whole spectrum of the criminal justice system, including female experts, who should be involved at the national level in the prevention and investigation of cybercrime.

58. Awareness-raising and educational campaigns and initiatives, including those covering emerging threats and those targeted at specific audiences such as children, were highlighted as an important component of policies to prevent cybercrime. In that context, it was emphasized that priority should be accorded to fostering a “cybersecurity culture” in order to strengthen the awareness of all actors of the criminal risks and threats posed by cybercrime, as well as to develop a common understanding of the necessary security and preventive measures.

59. It was stressed that cybersecurity awareness, in particular cybercrime risks and the dark side of the Internet, should be included as a subject in primary, secondary and tertiary education, for both students and teachers. It was added that that should

ideally be part of a national cybersecurity strategy. Some speakers placed emphasis on the need to prevent the spread of hate speech, extremism and racism, as well as cyberbullying and online violence, including gender-based violence and violence against vulnerable groups, through either educational initiatives or streamlining existing regulatory frameworks, or both. In addition, one speaker was of the view that States should devote special attention to preventive measures aimed at youth, including first-time offenders, in order to prevent reoffending.

60. One speaker shed light on the need for tools to guarantee the security of digital commerce, considering that that subject needed to be inserted into a broader development agenda for countries that did not yet fully benefit from that way of conducting trade in goods and services.

61. Intelligence analysis and criminological research were mentioned as important tools for the prevention of cybercrime. Reference was made to the analysis of large volumes of open source information (cyberpatrols) as a method to identify threats and vulnerabilities, analyse their scope and impact and respond at an early stage with alerts, guides and training.

62. One speaker referred to the work of INTERPOL with public and private partners to develop sound cybercrime strategies, including by running global awareness-raising campaigns to support law enforcement entities in overcoming the challenges of tacking cybercrime and the underreporting thereof.

63. One speaker reported on the work carried out under the "No More Ransom" project, a joint initiative of law enforcement agencies and information and technology security companies to disrupt cybercriminal businesses with ransomware connections and to help victims of ransomware retrieve their encrypted data without having to pay the criminals. The same speaker referred to the European Crime Prevention Network for the exchange of cybersecurity and safety policy best practices.

C. Other matters

64. At its 6th meeting, on 29 July 2020, the Expert Group considered agenda item 4, entitled "Other matters". No matters were raised under the agenda item.

IV. Organization of the meeting

A. Opening of the meeting

65. The meeting was opened by Doctor Mashabane (South Africa), Chair of the Expert Group, who delegated André Rypl (Brazil), Vice-Chair of the Expert Group, to chair the meeting on his behalf.

B. Adoption of the agenda and other organizational matters

66. At its 1st meeting, on 27 July 2020, the Expert Group adopted the following provisional agenda:

1. Organizational matters:
   (a) Opening of the meeting;
   (b) Adoption of the agenda.
2. International cooperation.
3. Prevention.
4. Other matters.
5. Adoption of the report.

C. Statements

67. Statements were made by experts from the following Member States: Algeria, Argentina, Armenia, Australia, Austria, Azerbaijan, Brazil, Canada, China, Chile, Colombia, Cuba, Dominican Republic, Ecuador, Egypt, Estonia, France, Germany, Greece, Guatemala, Honduras, Hungary, India, Indonesia, Iran (Islamic Republic of), Iraq, Israel, Italy, Japan, Lebanon, Malaysia, Mexico, Mongolia, Netherlands, New Zealand, Nigeria, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Romania, Russian Federation, South Africa, Spain, Thailand, United Kingdom, Venezuela (Bolivarian Republic of), Viet Nam and United States.

68. A statement was made by an expert from the State of Palestine, a non-member observer State.[2]

69. Statements were also made by representatives of the following intergovernmental organizations: Council of Europe, European Union and INTERPOL. A statement was made by an observer from the Beijing Normal University.

D. Attendance

70. The meeting was attended by representatives of 93 Member States, a non-member observer State, an institute of the United Nations crime prevention and criminal justice programme network, intergovernmental organizations and the private sector.

71. A provisional list of participants was circulated at the meeting (UNODC/CCPCJ/EG.4/2020/INF/1).

E. Documentation

72. The Expert Group had before it, in addition to the comments from Member States received in accordance with the workplan for the period 2018–2021, the annotated provisional agenda (UNODC/CCPCJ/EG.4/2020/1).

V. Adoption of the report

73. At its 6th meeting, on 29 July 2020, the Expert Group adopted the present report.

[2] The observer for the State of Palestine also made a statement on behalf of the Group of 77 and China.