17 January 2021
English
Original: All languages

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 6–8 April 2021

Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020

Conference room paper prepared by the Secretariat

I. Introduction

1. The present conference room paper contains a compilation of all preliminary conclusions and recommendations suggested by Member States during the past Expert Group meetings in 2018, 2019 and 2020. At each year's meeting a list of preliminary conclusions and recommendations suggested by Member States was prepared by the Rapporteur, with assistance from the Secretariat and based on the discussions and deliberations of the Expert Group.

2. This year's Expert Group stock-taking meeting will finish consideration of all the preliminary conclusions and recommendations and will produce a consolidated list of adopted conclusions and recommendations for submission to the CCPCJ.

3. The aim of this conference room paper is to circulate all the preliminary conclusions and recommendations to Member States, observers and other stakeholders prior to the stock-taking meeting for comments. Those comments should be posted online in advance of the stock-taking meeting for consideration by delegations.

V.21-01012 (E)

II. Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018

A. Legislation and frameworks

4. 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 "Legislation and frameworks". These preliminary recommendations and conclusions were submitted by Member States and their inclusion does not imply their endorsement by the Expert Group:

(a) Member States should ensure that their legislative provisions withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used. Member States should also consider establishing consistent terminology to describe cybercrime activities and facilitate, to the extent possible, accurate interpretations of relevant laws by law enforcement agencies and the judiciary;

(b) Member States should respect the sovereign rights of other States in formulating policies and legislation that meet their national conditions and needs in addressing cybercrime. To foster international cooperation to combat cybercrime, the principle of national sovereignty should not mistakenly be interpreted as an obstacle, but rather be considered fundamental and regarded as a starting point. The volatile nature of electronic data transmission and storage, such as in so-called clouds, may require engaging in multilateral discussions on innovative and expanded mutual assistance between States to ensure timely access to electronic data and evidence;

(c) To prevent and/or eliminate safe havens for criminals, Member States should cooperate with each other to the widest extent possible in investigations, evidence collection, prosecution, adjudication and, where necessary, the removal of illegal content from the Internet. Member States should also offer the greatest degree of flexibility possible in their international cooperation to combat cybercrime and other crimes involving electronic data, either when leading investigations or when sharing evidence, irrespective of whether the underlying activities are denominated differently in the respective States. In doing so, Member States should bear in mind that dual criminality is usually required for extradition but not necessarily for mutual legal assistance;

(d) In formulating policies and legislation, Member States should consider the need to strike a balance between human rights protection on the one hand, and national security, public order and the legitimate rights of third persons on the other. National legislations that criminalize conduct associated with cybercrime and grant procedural authority to investigate, prosecute and adjudicate on cybercrime cases should be consistent with due process guarantees, privacy interests, civil liberties and human rights. National policies and legislations as well as existing and/or future international instruments should follow a multidimensional approach. On the one hand, they should include adequate cybercrime policies based on a comprehensive understanding of the broader concept of cybersecurity. On the other hand, they should not only cover illegal conduct, but also focus on crime prevention and provide help to victims of crime and assistance to the general public. In order to create a solid base for international cooperation on combating cybercrime, Member States should strive to find and promote a culture of establishing a common future for cyberspace;

(e) Member States should pursue international cooperation without requiring full harmonization of national legislation, provided that the underlying conduct is criminalized and laws are sufficiently compatible to simplify and expedite the various forms of such cooperation;

(f) Member States should take into account that domestic legal frameworks continue to have a decisive function in ensuring the effectiveness and overall balance

of the system of investigation and prosecution, because criminal law is particularly sensitive in regard to fundamental rights and because investigations in the area of computer crimes concern, to a large extent, the private communications and data of citizens;

(g) To enable the prosecution of criminal acts, Member States should legislate on extraterritorial jurisdiction over citizens and persons ordinarily resident on their territory, irrespective of where those acts were committed and whether they constitute offences in the foreign jurisdiction;

(h) Member States may draw on different legal bases for international cooperation, including reciprocity, bilateral or multilateral treaties and other arrangements. Moreover, Member States with more advanced capacities and infrastructure in the field of cybercrime should assume responsibilities proportionate to those capacities or infrastructure in providing legal assistance to other States;

(i) To ensure that relevant issues are properly considered, Member States should consult all relevant stakeholders, including intergovernmental stakeholders, the private sector and civil society, as early as possible when the decision is made to introduce cybercrime legislation;

(j) Member States should foster strong and trustworthy public-private cooperation in the field of cybercrime, including cooperation between law enforcement authorities and communication service providers. Engaging in a dialogue with private industry, accompanied by public-private partnerships where possible and memorandums of understanding where needed, is also required to strengthen and facilitate cooperation;

(k) Member States should support UNODC in establishing an educational project or programme that focuses on raising awareness of cybercrime and appropriate responses to it among judicial and prosecution authorities, digital forensic experts of Member States and among private entities, and use capacity-building tools or an electronic knowledge management platform to raise awareness of the impact of cybercrime among civil society;

(l) Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by capacity-building measures and technical assistance programmes. Member States should allocate appropriate resources for domestic capacity-building. The proper implementation of cybercrime-related legislation requires the training of police and prosecutors, as well as public awareness campaigns. Such resources will also further international cooperation, as such cooperation is enhanced by a country's domestic capacity to investigate and prosecute cybercrime-related offences;

(m) Member States should strengthen existing frameworks and networks for combating cybercrime by identifying and addressing the weak points of those frameworks and networks and providing them with the necessary resources so as to improve their effectiveness;

(n) UNODC should engage actively in capacity-building for all Member States in need of assistance, in particular developing countries. Such capacity-building activities should be politically neutral and free from conditions, should result from thorough consultations and be voluntarily accepted by the recipient countries. In terms of substance, those capacity-building activities should cover at least the following areas:

(i) Training for judges, prosecutors, investigators and law enforcement authorities in cybercrime investigations, the handling of electronic evidence, chain of custody and forensic analysis;

(ii) Drafting, amending and/or implementing legislation on cybercrime and electronic evidence;

(iii) Structuring cybercrime investigation units and providing guidance on related procedures;

(iv) Drafting, updating, and implementing legislation to combat the use of the Internet for terrorist purposes;

(o) UNODC should seek synergies and cooperate closely with other stakeholders or organizations such as the Council of Europe and the Organization of American States (OAS) in the field of capacity-building programmes on combating cybercrime to ensure that activities and initiatives in this area are not dispersed or fragmented;

(p) Member States should continue to use the Expert Group as a platform for the exchange of information and best practices, including model laws or model clauses, relating to such issues as jurisdiction, special investigative techniques, electronic evidence, including challenges posed by the volatile nature of electronic evidence and its admissibility in court, and international cooperation;

(q) To avoid fragmentation, Member States should explore universally accepted practices and rules through multilateral consultation under the auspices of the United Nations and through the Expert Group platform;

(r) Member States should evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on a regular basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(s) Member States should develop a new international legal instrument on cybercrime within the framework of the United Nations that takes into account the concerns and interests of all Member States;

(t) Member States should use and/or join existing multilateral legal instruments on cybercrime such as the Council of Europe Convention on Cybercrime (Budapest Convention), as they are considered by many States to be best practice models guiding appropriate domestic and international responses to cybercrime;

(u) Existing legal instruments and mechanisms, including the United Nations Convention against Transnational Organized Crime, should be taken advantage of by as many States as possible to strengthen international cooperation;

(v) Under the auspices of the Expert Group, Member States should explore internationally applicable responses that could be reflected in model laws or model clauses where appropriate, and in doing so should draw on best practices in existing regional instruments and/or national legislation.

B. Criminalization

5. 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 “Criminalization”. These preliminary recommendations and conclusions were submitted by Member States and their inclusion does not imply their endorsement by the Expert Group:

(a) Member States should take into account that many substantive criminal law provisions designed for “offline” crime may also be applicable to crimes committed online. Therefore, to strengthen law enforcement, Member States should use existing provisions in domestic and international law, as appropriate, to tackle crimes in the online environment;

(b) Member States should adopt and apply domestic legislation to criminalize cybercrime conduct and to grant law enforcement authorities procedural authority to investigate alleged crimes consistent with due process guarantees, privacy interests, civil liberties and human rights;

(c) Member States should continue to enact cyber-specific criminal legislation that takes into account new criminal conduct associated with the misuse of information and communications technology to avoid relying on generally applicable provisions of criminal law;

(d) Member States should criminalize core cybercrime offences that affect the confidentiality, integrity and availability of computer networks and computer data, taking into account widely recognized international standards;

(e) Cyber-related acts that are minor infringements rather than criminal offences should be addressed by civil and administrative regulations as opposed to criminal legislation;

(f) To the extent that they have not done so already, Member States should consider the criminalization of:

(i) New and emerging forms of cybercrime activities such as the criminal misuse of cryptocurrencies, offences committed on the darknet and the Internet of things, phishing, and the distribution of malware and any other software used for committing criminal acts;

(ii) The disclosure of personal information and “revenge porn”;

(iii) The use of the Internet to commit acts related to terrorism;

(iv) The use of the Internet to incite hate crime and violent extremism;

(v) The provision of technical support to or assistance in the perpetration of an act of cybercrime;

(vi) The establishment of illicit online platforms or the publication of information to perpetrate cyber-related crimes;

(vii) Illegally gaining access to or hacking into computer systems;

(viii) Illegally intercepting or damaging computer data and damaging computer systems;

(ix) Illegally interfering with computer data and systems;

(x) Misuse of devices;

(xi) Computer-related forgery and fraud;

(xii) Child sexual abuse and exploitation;

(xiii) The infringement of copyrights;

(xiv) Child sexual abuse and exploitation, and incitement of minors to commit suicide;

(xv) Unlawfully influencing critical information infrastructure;

(g) Member States should ensure that computer-specific offences are drafted as tailor-made provisions that do not simply extend the application of traditional offences to the digital environment, but take into account the special features of the digital environment and the actual need for criminalization based on a careful assessment;

(h) Member States should bear in mind that the focus of international harmonization concerning criminalization of cybercrime should be on a core set of offences against the confidentiality, integrity and accessibility of information systems, while a need to harmonize criminalization concerning general offences that are committed using information and communications technology should mainly be dealt with in specialized forums concerning specific areas of crime;

(i) Member States should avoid criminalizing a broad range of activities by Internet service providers (ISPs), especially where such regulations may improperly limit legitimate speech and the expression of ideas and beliefs. Member States should

instead work with ISPs and the private sector to strengthen cooperation with law enforcement authorities, noting in particular that most ISPs have a vested interest in ensuring that their platforms are not abused by criminal actors;

(j) Member States should adopt and implement domestic legal evidence frameworks to permit the admission of electronic evidence in criminal investigations and prosecutions, including the appropriate sharing of electronic evidence with foreign law enforcement partners;

(k) Member States should use the Organized Crime Convention to facilitate the sharing of information and evidence for criminal investigations relating to cybercrime, given the frequent involvement of organized crime groups in cybercrime;

(l) Member States should explore ways to help to ensure that the exchange of information among investigators and prosecutors handling cybercrime is made in a timely and secure way, including by strengthening networks of national institutions that may be available 24/7;

(m) On the issue of criminalizing ISP non-compliance with law enforcement, Member States should exercise caution and pay meticulous attention to the detrimental effects on private sector activities and fundamental human rights, in particular freedom of speech;

(n) In effectively addressing cybercrime, Member States should take into consideration existing human rights frameworks, in particular as regards freedom of expression and the right to privacy, and should uphold the principles of legality, necessity and proportionality in criminal proceedings relating to the fight against cybercrime;

(o) Member States should identify trends in the activities underlying cybercrime through research and should further evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on an annual basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(p) Member States should consider the adoption of comprehensive strategies against cybercrime that include developing victimization surveys and informing and empowering potential victims of cybercrime;

(q) Member States should consider taking further preventive measures against cybercrime including, but not limited to, measures for the responsible use of the Internet, especially by children and young people.

III. Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019

A. Law enforcement and investigations

6. 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

7. 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.

IV. Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 July 2020

A. International cooperation

8. 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;

(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

[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 (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).

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 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

9. 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.