IEG on Cybercrime – Australian Comments ahead of the stocktaking meeting – Vienna, April 2021

Australia thanks the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime (the IEG) for its work in compiling the list of State recommendations submitted to the IEG over its preceding three meetings in 2018, 2019 and 2020. Australia takes this opportunity to provide specific comments on selected recommendations (Part 1). We also provide detailed comments on the broader issue of maintaining a Vienna-based forum for technical exchange and capacity building (Part 2).

Part 1: Comments on IEG recommendations

General comments

1. Australia acknowledges and accepts the passage of UNGA Resolution 74/247. During the discussion of 74/247, Australia, along with many other Member states, reiterated its view that a new UN convention on cybercrime was not required for States to make progress combatting cybercrime and its impacts on society. Despite these arguments, the mandate of the Ad Hoc Committee established by Resolution 74/247 passed by a recorded vote. Following the will of the General Assembly, Australia will respect the work and mandate of the Ad Hoc Committee, but it is important that the IEG's report does not now imply consensus on this issue where none exists. The views of the many member States which identified the effectiveness of utilising existing instruments, including the United Nations Convention against Transnational and Organised Crime and the Council of Europe Budapest Convention on Cybercrime (the Budapest Convention), remain valid and the passage of 74/247 does not change that.

2. The nature of cybercrime and State responses continue to evolve rapidly and have done so across the duration of the IEG's mandate. It will be important that the report reflect that the recommendations and conclusions collated for the study provide a snapshot in time against a background which is continually changing and raising new and difficult issues. Accordingly, the IEG's recommendations and conclusions may not necessarily reflect efforts to modernise existing international instruments, such as the draft Second Additional Protocol to the Budapest Convention.

3. Australia notes the impact of the COVID-19 pandemic on the 2020 meetings of the IEG and its outcomes (International Cooperation and Prevention) which prevented discussion of recommendations by States (in contrast with previous meetings) and instead resulted in a simple list of every recommendation put forward by a Member States. On this basis, Australia has provided more detailed comments on conclusions and recommendations submitted at those sessions.

Duplication of issues dealt with under other UN initiatives on Cyberspace and International Peace and Security

4. Australia is concerned that several recommendations fall outside the scope of cybercrime and the criminal misuse of ICTs. Issues related to information and communications technologies in the context of international peace and security – including the behaviour of States, the application of existing international law and agreed norms, the protection of critical infrastructure from malicious cyber activity, and malicious cyber activity conducted by States or their proxies and possible

responses thereto – are duplicative of the discussions among all 193 UN Member States in the UN First Committee Open Ended Working Group, which concluded its report on 12 May; the new 5-year Open Ended Working Group, which will begin its work in June, as well as the Groups of Governmental Experts on Cyber. Australia therefore objects to the inclusion of the following recommendations on the basis that they relate to matters of international peace and stability and fall outside the mandate of the IEG and the Third Committee recommendations 8(f), (h), (m), (ee)(iii) under International Cooperation and recommendations 9(g), (u), (kk), (ll), (nn), (pp) under Prevention.

Legislation and frameworks

5. The critical importance of ensuring legislation and frameworks are contemporary, technology neutral and appropriately criminalise the underlying conduct must be underscored – these elements form the basis of a State's national response to cybercrime and are essential precursors for international cooperation. As is the case with all criminal laws and legislative frameworks, careful consideration must be given to ensuring a balanced approach to law enforcement, human rights and privacy issues, ensuring compliance with member States' human rights obligations. Close consultation with civil society, industry and relevant stakeholder is critical in general, but particularly so in this regard. Public-private partnerships will continue to be essential to detecting, preventing and obtaining electronic evidence to investigate and prosecute cybercrime. Given the transnational nature of cybercrime and the need to eliminate safe havens for criminals, extraterritorial jurisdiction should be applied to cybercrimes, in accordance with international law.

6. Conclusions should underscore the importance of a 'system wide' approach to criminal justice. Legislation and frameworks for cybercrime must provide for, and be accompanied by, appropriate powers, procedures, capabilities and capacity across the entire justice system, including law enforcement, central authorities, prosecutorial authorities, and the judiciary.

7. Member states should take advantage of existing international frameworks which provide for effective international cooperation cybercrime including the Council of Europe Convention on Cybercrime (Budapest Convention) and the United Nations Convention Against Transnational and Organised Crime.

8. Commentary on Australia's support for continuation of technical and expert exchange, including through the IEG, is addressed in Part 2, below.

In line with these general comments, Australia strongly supports the intent of the following recommendations and conclusions:

- 4(a),(d),(e), (g), (i), (j), (t), (u).
- In line with our comments on human rights, privacy, and good governance Australian also supports the intent of recommendation 5(n), currently listed under Criminalization
- In line with our comments on contemporary legislative frameworks which are technology neutral, Australia also supports the intent of recommendation 6 (j) currently listed under Law Enforcement and Investigations
- In line with our comments on the benefits of utilising existing international frameworks to cooperate on cybercrime Australia also supports the intent of recommendations 6 (b), (c), and (d) currently listed under the Law Enforcement and Investigations

Criminalization

9. Criminalisation of conduct constituting cybercrime is fundamental to national and international efforts to combat cybercrime. This should include key offences relating to the confidentiality, integrity and availability of computer networks and computer data and should take into account widely recognized international standards. In order to be effective, law enforcement must be appropriately empowered and equipped to undertake cybercrime investigations. An often overlooked, but critical aspect of an effective criminal justice response to cybercrime is the maintenance of appropriate arrangements for obtaining, management and handling, judicial consideration and international cooperation on electronic forms of evidence.

In line with these comments, Australia strongly supports the intent of the following recommendations and conclusions:

- 5(b), (d), (j), (l).

Law Enforcement and Investigations

10. The rapid pace and cross-border nature of cybercrime pose challenges for traditional regulatory and law enforcement approaches. The capacity and capabilities of our agencies, particularly law enforcement agencies, need to keep pace with evolving technologies if police are to perform their duties in the digital environment. At the most basic level, all police officers need to know how to gather and analyse digital evidence, leaving specialist units to focus on more complex cybercrimes. Specialist units within law enforcement agencies must have the training and capabilities to detect and investigate the more complex and sophisticated use of technology in criminal activities.

In line with these comments, Australia strongly supports the intent of the following recommendations and conclusions:

- 6(h), (I), (k), (n).
- In line with our comments on capacity, capability and specialisation of criminal justice agencies to effectively combat cybercrime, Australia also supports the intent of recommendations 8(ccc), (ddd).

Electronic Evidence and Criminal Justice

11. The use of online and cloud computing services has become integral to communication in daily life. From a criminal justice perspective, this makes them key sources of evidence for prosecuting both traditional and online crime. However, the successful prosecution of individuals who commit crimes involving electronic evidence relies on:

- appropriately skilled and resourced law enforcement agencies and forensic practitioners who are able to collect, analyse and present the evidence;
- a legislative framework that facilitates the collection, presentation and adjudication of evidence in the modern era, noting that relevant electronic evidence may be stored beyond the jurisdiction of the investigating law enforcement agency, and the nation's borders generally; and
- appropriately trained prosecutorial, judicial and central authorities that can work efficiently and effectively with electronic evidence.

12. Australia recognises the importance of capacity building, collaboration and international cooperation, and exchange on trends and best practices for combatting cybercrime. Our views on the best forum to address this ongoing need are outlined in Part 2 of this paper.

In line with these comments, Australia strongly supports the intent of the following recommendations and conclusions:

- 7(b), (c), (d), (f), (g), (o)(i-vi), o(viii), o(xii-xv), (r), (v).

International cooperation

13. Australia agrees with recommendations and conclusions advocating that Member States be encouraged to use international treaties and arrangements already in existence, such as the Budapest Convention. The Budapest Convention provides a foundational substantive and procedural legal framework that enhances the ability to combat cybercrime and the collection of electronic evidence more broadly.

14. Member States should also be informed of efforts to modernise existing international treaties, such as the Budapest Convention. Currently, the Budapest Convention Cybercrime Committee (T-CY) are negotiating the Second Additional Protocol on enhanced cooperation and disclosure of electronic evidence. This will significantly improve the ability for Parties to both directly and indirectly obtain electronic evidence to combat all manner of crime types (including cybercrime) and facilitate more effective international cooperation (such as joint investigations).

Terminology and definitions

15. Efforts to define 'cybercrime' should focus on technology-neutral language to ensure that the recommendations and conclusions are relevant and accessible to all jurisdictions despite the constant evolution of technologies.

16. Australian notes recommendation (8(a) International Cooperation) refers to 'child pornography.' Member States should be encouraged to replace references to 'child pornography' as with more appropriate alternative terms, such as 'child sexual abuse material.' Similarly, the Member States should be encouraged to use alternative terminology such as 'non-consensual sharing of intimate images' in place of references to 'revenge porn', as included in recommendation 5(i)(ii).

Capacity building and technical assistance

17. Recommendations and conclusions should foster international cooperation, confidence building and trust between countries to ensure that criminal justice practitioners have effective and efficient ways to detect, prevent, investigate and prosecute cybercrime.

18. Capacity building and technical assistance are an important feature of international cooperation and building global resilience – the response to cybercrime is only as strong as our collective efforts. The need for appropriate capacity building programs, particularly for developing countries and small island states, is a key theme of conclusions and recommendations across the IEG's thematic meetings. Australia strongly supports the UNODC's role in the provision of capacity building and expertise on cybercrime, including through its Global Programme on Cybercrime. Capacity building programs should adopt a system-wide approach and include support for the development of relevant cybercrime legislation and frameworks.

19. International efforts should focus on the provision of capacity building and technical assistance to strengthen the ability of law enforcement authorities to combat cybercrime, especially child sexual abuse online.

20. Commentary on Australia's support for continuation of technical and expert exchange, including through the IEG, is included in Part 2, below.

Investment in international crime cooperation

21. Member States should be encouraged to invest in central authorities to ensure effective international crime cooperation, including by ensuring there is sufficient expertise to respond to emergency requests and securing the preservation of data to reduce the risks associated with data loss/volatility. Central authorities should also be supported through mechanisms such as 24/7 networks in law enforcement or specific contact points in central authorities, to ensure mutual legal assistance can be provided to the widest extent possible.

Domestic procedural frameworks and international cooperation

22. Government access to data for law enforcement purposes should be supported by frameworks that ensure the preservation of electronic evidence – such as the preservation procedural measures of the Budapest Convention. Collective consideration should also be given to ensure law enforcement and national security agencies lawful access to end-to-end encrypted data is maintained on messaging platforms, to support the prevention, detection, investigation and prosecution of criminal offences.

23. There are many challenges with the current status quo in terms of international cooperation. Member States should be encouraged to consider how international cooperation can be improved and made more effective.

24. Member States should be encouraged to strengthen their own law enforcement capabilities to combat cybercrime, including through establishing specialised expertise within law enforcement and prosecutorial authorities to investigate and prosecute cybercrime.

Public and private partnerships

25. Member States should be encouraged to support the position that criminality on the internet is not only the responsibility of governments, but also shared with industry. This includes the need for industry to develop policy, codes and practices in responding to the criminal use of their networks and services. Broader education efforts will be necessary to give effect to this position.

26. Public-private partnerships are critical to detecting, preventing and obtaining electronic evidence to investigate and prosecute cybercrime. This includes public-private partnerships that ensure lawful access is maintained to end-to-end encrypted data on messaging platforms.

27. Member States should be encouraged to engage with domestic and international service providers that provide services to their jurisdiction, to ensure there is open dialogue around how Member State authorities can obtain electronic evidence (including through international cooperation mechanisms such as mutual legal assistance).

In line with the above comments, Australia strongly supports the intent of the following recommendations and conclusions:

- 8 (a), (c), (e), (p), (r), (s), (t), (u), (w), (z), (bb), (hh), (jj), (ll), (pp), (rr), (uu), (aaa), (ggg).
- In line with our comments on capacity building, Australia also supports the intent of recommendation 4(n) under Legislation and Frameworks, 6(e), (f), and (t) under Law Enforcement and Investigations.

In line with our general comments, above, Australia could not support the following recommendations:

- 8 (f), (h), (m), (ee)(iii).

Prevention

28. Australia agrees that prevention is not only the responsibility of governments but requires the participation of all relevant stakeholders, including industry and the public.

29. Australia supports the recommendations and conclusions regarding the development of initiatives to better equip the public to protect themselves against cybercrime, including accessible prevention tools and public awareness campaigns for the safe and legal use of the internet.

30. Australia supports recommendations to move to a more proactive prevention posture, including greater and more routine information sharing between Member States on criminal *modi operandi*.

31. Australia supports the development of strategies and measures to ensure prevention keeps pace with advances in technology, such as the criminal use of anonymising tools. For example, Australia supports efforts to prevent terrorist and violent extremist use of the internet through working with governments, industry and civil society.

32. Australia supports greater sharing of international best practice on effective and successful prevention of cybercrime (such as through the IEG).

In line with the above comments, Australia strongly supports the intent of the following recommendations and conclusions:

- 9(a), (b), (v), (w), (y), (z), (aa), (gg).
- In line with our comments on public awareness and prevention tools, Australia supports recommendation 5(q) under Criminalization.

In line with our general comments, above, Australia could not support the following recommendations:

- 9 (g), (u), (kk), (ll), (nn), (pp).

Part 2: The need for an ongoing forum for technical exchange

25. The original mandate of the Intergovernmental Expert Group on Cybercrime (IEG), established in UNGA Resolution 65/230, set out a two-pronged mandate for the IEG's work:

> *Requests* the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration, 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.[1]

26. That mandate specified the IEG's primary objective as the completion of a comprehensive study of the problem of cybercrime and responses to it by Member States. As part of that mandate, it also included a request that the IEG facilitate 'the exchange of information on national legislation, best practices, technical assistance and international cooperation', with a view to improving the international response to cybercrime.

27. That technical exchange element has been one of the most important and enduring benefits of the IEG's work. The IEG forum has enabled states to canvass a range of technical and practical issues related to combatting cybercrime, encouraged meaningful exchange at a practitioner-level, and ensured States continue to benefit from the high degree of expertise and experience gathered in Vienna, as well as the resources of the UNODC and its Global Program on Cybercrime.

28. To enhance Member States' ongoing ability to share information, continue practitioner-level technical engagement and foster technical assistance and capacity building, this element of the IEG's work must endure, whether under the auspices of the IEG or in a different format.

Longstanding consensus on the need for ongoing technical exchange

29. Despite their divergent views on the value of new international instruments, States have long agreed on the value of the IEG's technical exchange function as a distinct component of its broader mandate. As early as the first meeting of the IEG in 2011, a number of States:

> 'highlighted the importance of technical assistance and information-sharing, both under the auspices of a comprehensive international legal instrument and on the basis of more immediate needs and means of delivery. It was noted that the same issue was identified as a separate and specific priority by the Salvador Declaration'.[2]

30. At the second meeting of the IEG in 2013, experts again:

> 'highlighted the importance of effective ongoing communications between States in order to share and address concerns about specific cases and increase understanding of what barriers existed and how they could be addressed'.[3]

31. The CCPCJ reaffirmed this broad agreement on the value of technical exchange and capacity-building in its resolution 22/7, when it underlined 'the need for enhanced coordination and cooperation among States in combating cybercrime'[4]. The CCPCJ also confirmed in its resolution

---

[1] A/RES/65/230, OP9.
[2] Paragraph 31, UNODC/CCPCJ/EG.4/2017/2.
[3] Paragraph 37 CCPCJ/EG.4/2017/3.
[4] E/2013/30, p62.

22/8 the 'broad support for capacity-building and technical assistance and for the role of the UNDOC in that regard'.[5]

32. In response to a recommendation of the Doha Declaration, CCPCJ resolution 26/4 extended the mandate of the IEG and gave it the framework for its current work plan. In so doing, the CCPCJ specifically highlighted the separate importance of the IEG's work in facilitating technical exchange [emphasis added]:

> *Requests* [the IEG] to continue its work … *and also requests* 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.[6]

33. In subsequent meetings of the IEG, States have repeatedly stressed the need for an ongoing facility for technical exchange, with at least eight separate recommendations highlighting the need for ongoing technical exchange and capacity building among States.[7]

34. Australia considers the IEG remains a critical forum for experts and practitioners to exchange information on their experiences and ongoing efforts to combat the ever-increasing threat of cybercrime, and that such exchange should continue beyond 2021.

Options for ongoing technical exchange

35. Given the longstanding and widely-held support among States for an ongoing forum for expert and technical exchange, it is important to consider the most effective way to meet this need.

36. In Australia's view, the IEG, as an established body with an existing UNGA mandate, is the forum best equipped to continue to facilitate international technical exchange. Once the comprehensive study on cybercrime is complete at the end of 2021, States could easily adapt the IEG's mandate to focus solely on technical exchange, capacity building, and the identification and analysis of trends in cybercrime.

37. Alternatively, States may prefer to establish a new platform for discussions rather than adapt an existing one. If so, such a platform could be established as a separate mechanism, process or forum. As with the IEG, any new forum should be established in Vienna, under the auspices of the CCPCJ, to ensure States can continue to benefit from the expertise, experience and resources available in Vienna and in the UNODC. Such an arrangement would ensure States continue to have meaningful opportunities for technical exchange and capacity building.

38. It should be stressed that the Ad Hoc Committee (AHC) established by UNGA resolution 74/247 is not a suitable forum to facilitate the kind of technical and expert-led exchange that currently occurs under the auspices of the IEG, having neither the mandate nor the resources required. Rather, the AHC's mandate is limited by the narrow terms of 74/247, to the elaboration of 'a comprehensive international convention on countering the use of information and communications technologies for criminal purposes'.[8]

---

[5] Ibid, p65 (OP1).
[6] E/2017/30, p 34 (OP1).
[7] See for example recommendations 4(p); 4(q); 5(l); 5(o); 7(i-l); 7(o); 8(rr); and 9(xx) in UNODC/CCPCJ/EG.4/2021/CRP.1.
[8] A/RES/74/247, OP2.

39. In view of the AHC's status as a subsidiary body of the General Assembly, it would not be appropriate for the CCPCJ to attribute to the AHC functions which were not within its existing mandate. In addition, Australia's considers matters relating to criminal justice, including cybercrime, should be dealt with under the auspices of UN's Vienna based institutions, the home of criminal justice in the UN system. To continue facilitating these essential technical discussions, States must either make use of the tools already available to them (the IEG) or create new dedicated/tailor-made/purpose-built ones. Irrespective of the mechanism under which States choose to continue much needed technical and expert exchange, duplication and overlap with other processes should be avoided.

Permanent
Mission
of Austria

to the United
Nations in Vienna

Comments on Future Work of the
Intergovernmental Expert Group (IEG) on Cybercrime

Austria aligns with the EU comments on the future work of the Expert Group. In our national capacity, we wish to make some additional remarks.

Austria firmly supports the position that the Commission on Crime Prevention and Criminal Justice (CCPCJ) should renew the mandate of the Expert Group beyond 2021 as a platform for experts and practitioners in the field of cybercrime to exchange information and best practices.

Whether the IEG is extended in its current form or a new forum for facilitating this expert exchange is established, future meetings should take place in Vienna, as the hub for international cooperation in all criminal matters and combatting cybercrime in particular. The UN seat is host to the necessary expertise and can be considered a repository of knowledge on the subject.

The CCPCJ should continue to have leadership over the expert-driven forum. The United Nations Office on Drugs and Crime (UNODC) in Vienna is the right entity to take this work forward, both in terms of its mandate and its expert knowledge.

Furthermore, we are ready to actively engage in the new process of the Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. However, Austria does not hold the view that the negotiation of a new convention on cybercrime is comparable to the exchange among experts in the field, which has been made possible through the IEG. A Vienna-based platform is needed that is separate from the political discussions on cybercrime policies and that allows practitioners to connect and share practical experiences from around the world.

We look forward to a fruitful discussion on these matters at the seventh meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, which will be held in Vienna, Austria, from 6 to 8 April 2021.

Andromeda-Tower, 11th fl., Donau-City-Str. 6, 1220 Vienna
Tel.: (+43/1) 263 72 91-0. Fax: (+43/0) 501159-600; E-mail: ovwien@bmeia.gv.at

Canadian Comments on Future Work of the Intergovernmental Expert Group (IEG) on Cybercrime

Canada agrees with the recommendations made at previous sessions of the Intergovernmental Expert Group on Cybercrime (IEG) that the IEG should continue its important work. Since its establishment in 2011, the IEG has proven to be an invaluable forum to advance our shared interest of combatting cybercrime at a time when individuals and groups are increasingly using the internet to commit criminal acts. And now, more than ever, the United Nations needs a forum for experts to exchange information and experiences, and collaborate, including on the development of best practices, emerging criminal phenomena, the identification impediments to the investigation and prosecution of cybercrime, and the development of prevention and capacity building strategies. Canada agrees that the Commission on Crime Prevention and Criminal Justice (CCPCJ) should extend the mandate of the IEG beyond 2021 (recommendation IV A8rr).

Canada agrees that the IEG mandate needs to be revised bearing in mind the role of the open-ended ad hoc committee to elaborate a comprehensive international convention on cybercrime that was established in 2019 by United Nations General Assembly (UNGA) resolution A/RES/74/173. However, during that same session in 2019, UNGA also recognized the importance of the IEG as "an important platform for the exchange of 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 for cybercrime" (A/RES/74/173). Therefore, bearing in mind these two resolutions, the IEG should continue to serve as a non-political forum for information exchange and to inform the negotiation process. Cybercrime and the challenges presented by electronic evidence are complex issues that need to be discussed by experts in a specific, focused forum. The IEG has already made significant strides in a number of important areas that are globally recognized as priorities in the fight against cybercrime, including bringing domestic legislation in-line with international standards, and has resulted in innovative capacity building initiatives.

As suggested in recommendation II A4p, the IEG could continue to serve "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". Canada would also be interested in the IEG being mandated to conduct a regular assessment of cybercrime trends (II A4r, II B5o and III B7k) and assisting in drawing on best practices in existing instruments.

Should the IEG no longer be in a position to continue to perform its mandate, Member States must consider an alternative forum for expert exchange with the UN Office on Drugs and Crime (UNODC) facilitating and the CCPCJ guiding the work.

The Permanent Mission of the Canada is pleased to respond to the "*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.*" Canada greatly appreciates the opportunity to provide feedback on the preliminary conclusions and recommendations. Canada extends its compliments to the IEG on the work undertaken to develop these recommendations and would like to highlight, in particular, the recommendations listed below as those that Canada finds particularly important and proposes including in the final submission to the Commission on Crime, Prevention and Criminal Justice. Canada would also like to emphasize, once again, that Canada supports the IEG's continuation.

I. Legislation and Frameworks

Recommendations:

- 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 (II A4(d)).

- 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 (part of II A4(a).

- 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 (II A4(i)).

- Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by capacity-building measures and technical assistance programs. Member States should allocate appropriate resources for domestic capacity-building (part of II A4(l)).

- 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 (II A4(t)).

- 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 (II A4(u).

II. Criminalization

Recommendations:

- 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 (II B5(b)).

- 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 (II B5(d)).

- 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 (II B5(i)).

- 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 (II B5(n));

- 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 (II B5(j)).

- 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 (II B5(o)).

III. Law Enforcement and Investigations

Recommendations:

- 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 (part of III A6(b)).

- 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 (III A6(i)).

- 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, 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 (III A6(k));

- 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 (III A6(l)).

- Member 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 (III A6(r);

- 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 (III A6(c)).

IV. Electronic Evidence and Criminal Justice

Recommendations:

- 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 or multilateral treaty or in cooperation with the country that has jurisdiction (III B7(f)).

- 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 (III B7(c)).

- 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 (III B7(d)).

- 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 (III B7(e)).

- 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 and prosecutors;
  (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;
  (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;

(xiii) Strengthening of the technical and legal capacities of law enforcement agencies, judges and prosecutors through capacity-building and skill development programs; (xv) Holding of workshops and seminars to raise awareness of best practices in addressing cybercrime (part of III B7(o)).

- 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 (III B7(r)).

V. International Cooperation

Recommendations:

- 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 (part of IV A8(b)).

- International cooperation to combat cybercrime should also take into account gender- and age-sensitive approaches and the needs of vulnerable groups (IV A8(l)).

- 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 (IV A8(e));

- 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 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 (IV A8(hh)).

- 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 (IV A8(ddd)).

- 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 (IV A8(eee));

- 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 (IV A8(qq)).

- 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 (IV A8(t)).

- 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 (IV A8(u)).

- 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 (IV A8(rr)).

- 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 (IV A8(uu)).

- 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 international cooperation for many. Thus, countries should ensure that any new instrument on cybercrime avoids conflict with existing treaties (IV A8(ll)).

- 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 (IV A8(mm));

VI. Prevention

Recommendations:

- 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 (IV B9(e));

- 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 (IV B9(w)).

- Public-private partnerships, including cooperation with cybersecurity stakeholders and technology companies on information-sharing, are needed to prevent and combat cybercrime (IV B9(i)).

- “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 (IV B9(z)).

- Member States should avail themselves of capacity-building assistance from the UNODC Global Program on Cybercrime and other initiatives, including the Council of Europe Global Action on Cybercrime Extended programmes (IV B9(aa))

- 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 (IV B9(cc)).

- States should involve female experts in the prevention and investigation of cybercrime (IV B9(qq));

- 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 (IV B9(aa))

- Efforts in the development of strategies for cybercrime prevention should also take into account the protection of human rights (IV B9(y)).

附件

中国对联合国网络犯罪政府间专家组
第七次会议书面评论意见

一、一般性评论

中方支持并欢迎专家组按照2018年至2021年工作计划就网络犯罪有关实质问题开展的讨论。依据专家组第四至第六次会议讨论，秘书处汇编形成了初步结论和建议，有关建议全面反映了各国立足不同国情、不同法律制度和不同文化背景所实施的旨在预防、应对和打击网络犯罪的意见和举措，不仅有助于各国交流互鉴，也有助于强化打击网络犯罪国际合作。

由于会议模式、旅行限制等原因，专家组深入讨论汇编而成的结论和建议并予以通过将面临巨大挑战。第七次会议应当根据新形势，调整对会议成果的预期。如果各方无法就结论和建议达成一致并在第七会议上通过，可以考虑直接将秘书处准备的汇编提交给预防犯罪和刑事司法委员会，作为专家组的工作成果。相信这样的汇编对委员会、对各国也具有重要的参考价值。

第 74 届联大通过第 247 号决议，授权成立政府间特设委员会起草打击网络犯罪的全球性公约。这为各国强化合作、构筑全球打击网络犯罪网络提供了宝贵机会。各国应当积极参与和支持谈判进程，推动在联合国制定各方参与、包容开放的打击网络犯罪全球性公约。

关于网络犯罪有关问题，中方愿重申并强调如下：

（一）立法和框架

1、在国内层面，各国应立足网络数字技术迅猛发展和网络犯罪手段快速更新的现实，强化相关政策和立法，为预防和强化打击网络犯罪提供法律保障。

2、在国际层面，国际社会应高度重视网络犯罪的共同挑战，积极开展打击网络犯罪国际合作，在用好现有多双边合作机制和区域性打击网络犯罪平台的基础上，携手推动联合国打击网络犯罪公约特委会尽快启动实质谈判，为在全球范围内强化打击网络犯罪提供法律框架。

（二）定罪

1、加强对核心网络犯罪行为定罪的合作。可先将各国普遍关注并能达成共识的网络犯罪行为纳入国际合作的范畴，并根据实践不断补充。对于不能达成普遍共识的网络犯罪，也可按照国际合作的一般原则开展协作。

2、顺应当前网络犯罪发展趋势，适当扩大网络犯罪范畴。将

互联网用于恐怖主义目的的犯罪、利用网络从事赌博、诈骗、贩枪、儿童色情等犯罪、为他人实施网络犯罪提供技术支持或帮助的犯罪、为实施犯罪而设立非法网络平台等也加以定罪。此外，还应当将利用网络煽动仇恨犯罪，包括利用互联网煽动暴力、民族仇恨，教唆、引诱实施严重暴力犯罪，编造虚假信息故意在网络传播，危害公共安全和社会秩序等行为定罪。

（三）执法与调查

1、各国应重视加强对帮助行为、预备行为的调查和执法，以应对网络犯罪日益加剧的链条化趋势。

2、各国应就云计算、暗网、加密货币、物联网等对网络犯罪执法与调查的影响进行讨论，共同研究可行的应对之策。

3、鼓励各国通过立法明确网络服务提供者配合防范网络犯罪和协助执法与调查的义务。例如,鼓励网络服务提供者采取技术措施和其他必要措施，防范网络犯罪；制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，保障网络安全。

（四）电子证据与刑事司法

1、各国应制定或完善立法，承认电子证据的证据能力，规定电子证据的定义、范围、取证手段和采信规则等。同时，采取措施加强网络犯罪电子证据取证能力建设，培养法律素养和技术知识兼备的专业团队，加强在这方面的经验共享和培训合作。鼓励

联合国毒品和犯罪问题办公室在这一领域发挥作用。

2、各国跨国调取电子证据应尊重证据所在地的国家主权，遵守正当程序，尊重相关个人和实体的正当权利，不得采取侵入性和破坏性技术侦查手段跨国获取电子证据。

3、鼓励各国针对调查网络犯罪、调取电子证据的需要，协商通过优化程序等方法，进一步畅通司法协助和执法合作渠道。各国应考虑在打击网络犯罪全球性公约中纳入各方普遍接受的获取境外电子证据条款，为解决跨国调取电子证据问题提供统一、权威的指引。

（五）国际合作

1、各国应积极就打击网络犯罪开展国际刑事司法合作，包括引渡、协助调查取证以及预防和打击国际转移非法所得等。

2、各国确立对网络犯罪的管辖权应尊重他国主权，反对与犯罪缺乏真实、充分联系的过度域外管辖。鼓励各国加强沟通协商以解决管辖权的冲突。

3、各国应建立网络犯罪司法协助和执法合作快速联络响应机制和联系渠道，考虑通过采用电子签章等技术手段，实现跨境取证法律文书和电子证据网上交换，提高国际合作效率。对保全电子数据、提供日志信息等不涉及人身自由、财产权利，或对此类权利影响较小的协助调查取证请求，在不违反被请求国法律的前提下，被请求国应最大限度提供协助。

（六）预防

1、各国应将“预防为主，打防并重”作为打击网络犯罪的基本原则，根据网络犯罪的新特点制定有针对性的预防犯罪举措。

2、各国应立法明确规定网络服务提供者预防网络犯罪的义务，特别是安全风险预警、安全事件应急处置等义务。要求网络服务提供者一旦发现其服务被用于实施网络犯罪，立即采取阻断犯罪信息传播、关停钓鱼等涉案网站、关闭涉案域名等紧急处置措施。

3、各国应建立国际网络威胁信息共享机制，对新型威胁技术、作案手法及时共享、共同研究。

4、应加强对发展中国家的技术援助和培训，提升其预防网络犯罪的能力。

Comments by the People's Republic of China for the Seventh Meeting of the Open-Ended Intergovernmental Expert Group on Cybercrime

I. General Comments

China supports and welcomes the discussion of substantive issues of cybercrime by the Expert Group according to its work-plan for the period of 2018-2021. The preliminary conclusions and recommendations, compiled by the Secretariat based on discussions during the fourth to sixth meetings of Expert Group, fully reflect the suggestions and experiences of Member States in preventing and combating cybercrime, on the basis of different national situations, various legal systems and diverse cultural backgrounds. These recommendations could promote exchange of information, sharing of best practices and international cooperation on combating cybercrime.

Due to the modality of the seventh meeting and travel restrictions, it would be extremely difficult for the Expert Group to have in-depth discussion of all the preliminary conclusions and recommendations, not to mention their adoption. Bearing in mind the challenging situation, it would be advisable for Member States to lower their expectations for the outcome of the seventh meeting of the Expert Group. If a consolidated list of conclusions and recommendations could not be agreed, Member States may consider to submit the compiled preliminary conclusions and recommendations in its entirety to CCPCJ as the outcome of the Expert

Group. We believe that the preliminary conclusions and recommendations could also provide valuable reference to CCPCJ as well as Member States.

The 74th General Assembly adopted Resolution 74/247, which mandates the establishment of an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering cybercrime. It provides a valuable opportunity for States to facilitate international cooperation and build a global network on combating cybercrime. States should support and actively participate in this process to negotiate a global convention on countering cybercrime under the auspices of United Nations, adhering to universal-participation, inclusiveness and openness.

With respect to the substantive issues of cybercrime, China wish to reiterate and emphasize its position as follows:

1. Legislation and Frameworks

(i) At the national level, bearing in mind the rapid development of digital technologies and their exploitation by cybercrime perpetrators, States should improve relevant policies and legislations to provide legal framework for preventing and combating cybercrime.

(ii) At the international level, the international community should attach great importance to the common challenges of cybercrime, actively engage in the international cooperation on combating cybercrime. States should make good use of the existing multilateral and bilateral cooperation mechanisms and regional platforms for combating cybercrime, and work

together to support the UN Ad Hoc Committee to launch substantive negotiations in an earlier date, so as to provide a global legal framework for combating cybercrime.

2. Criminalization

(i) States should strengthen cooperation on criminalization of core cybercrime activities. States may include crimes that are of wide concern and consensus into the scope of international cooperation, and extend this scope continuously according to practice. For those cybercrimes cannot get consensus among States, assistance could be provided on the basis of general principles of international judicial cooperation.

(ii) Catering to the trend of current cybercrime, States should expand the scope of criminalization. States may criminalize such conducts, including using the internet for terrorism, gambling, fraud, trafficking of firearms, and child pornography, providing technical support or aid for cybercrime, setting up illegal internet platform for criminal purposes. In addition, using the internet to incite hate crimes, including inciting violence and hatred among different national groups, abetting and enticing others for serious violent crime, fabricating and spreading disinformation, and other activities jeopardizing public security and social order, should also be criminalized.

3. Law Enforcement and Investigation

(i) States should strengthen investigation and law enforcement actions against acts of aiding and preparation of cybercrime, so as to effectively

address the “supply chain” of cybercrime.

(ii) States should discuss the impact of cloud computing, dark web, cryptocurrency, the Internet of Things and other emerging technologies on law enforcement and investigation of cybercrime, and work together to find feasible solutions.

(iii) States are encouraged to establish in their domestic legislation Internet Service Providers’ obligation of assistance on prevention, investigation and law enforcement of cybercrime. For example, encouraging the ISPs to take technical and other necessary measures to prevent cybercrime, make emergency response plans for cybersecurity incidents, and deal with system bugs, computer viruses, network attack, network intrusion and other security risks in a timely manner.

4. Electronic Evidence and Criminal Justice

(i) States should enact or improve legislation to recognize the admissibility of electronic evidence, and provide for the definition, scope, collection methods and admissibility rule of electronic evidence. Meanwhile, States are encouraged to strengthen capacity-building for electronic evidence collection, establishing professional teams with legal and technical expertise, and enhance experience sharing and training cooperation in this regard. UNODC should be encouraged to play a role in this field.

(ii) When collecting electronic evidence abroad, States shall respect the sovereignty of States where data is located, comply with due process and respect the legitimate rights of relevant persons and entities, and shall refrain

from unilaterally using intrusive or destructive technical investigation measures in this regard.

(iii) States are encouraged to conduct consultation with other States to further improve international judicial assistance and enforcement cooperation by optimizing relevant procedures or other methods, to facilitate the investigation of cybercrime and collection of electronic evidence. States shall consider incorporating a provision on cross border electronic evidence collection in the future UN convention on combating cybercrime, in order to provide unified and authoritative rules to regulate activities of cross border electronic evidence collection.

5. International Cooperation

(i) States should conduct international criminal justice cooperation positively in areas such as extradition, assistance to investigation and evidence collection as well as prevention of and crackdown on international transfer of illicit gains etc.

(ii) States shall respect the sovereignty of other States when establishing jurisdiction over cybercrime, and should not exercise excessive extraterritorial jurisdiction which lacks sufficient and genuine link with the targeted cybercrime. States are encouraged to enhance communication and consultation to settle jurisdictional conflicts.

(iii) States shall establish a quick response mechanism and communication channel for judicial assistance and law enforcement cooperation in combating cybercrime, and consider enabling online

exchange of legal documents and electronic evidence supported by electronic signatures and other technical means. When dealing with requests of preservation of date and provision of log information, which do not involve personal freedom or property rights, and other request of investigation and evidence collection, which have minimal impact on the above mentioned rights, States should afford one another the widest measures of assistance in line with domestic law.

6. Prevention

(i) States should put prevention first, prioritize prevention and punishment in combating cybercrime, and take targeted preventive measures that cater to the emerging characteristics of cybercrime.

(ii) States shall define ISPs' obligations of preventing cybercrime in their domestic laws, in particular the obligation of early alert of cybersecurity risks and emergency response to cybersecurity incidents. ISPs, while detecting their services being used for criminal purposes, should be required to take emergency measures, including blocking the dissemination of illegal contents, shutting down phishing websites as well as other vicious websites, and blocking the involved domain names and etc.

(iii) States should establish an international mechanism for sharing cyber threat information, to facilitate timely sharing of information and coordinated research of the new threats of technologies as well as modus operandi of the criminals.

(iv) States are encouraged to provide technical assistance and training

to the developing countries with the aim of enhancing their capacity to prevent cybercrime.

二、专家组下步工作

中方欢迎并肯定专家组撰写的《网络犯罪问题综合研究报告》以及历次会议成果，感谢毒罪办作为专家组秘书处多年来为各国提供的大力支持。

目前，联合国已成立特委会，启动网络犯罪公约谈判进程，毒罪办也将作为特委会的秘书处，为各国参与公约谈判提供支持。启动公约谈判为各国进一步强化合作、应对网络犯罪提供了重要契机。各国应全力支持和参与特委会工作，尽早达成关于打击网络犯罪的新的全球性公约。考虑到特委会的工作即将于 2021 年 5 月启动，为避免重复劳动，使各国、特别是资源有限的发展中国家和毒罪办集中精力投入公约特委会的工作，专家组在按计划完成第七次会议的议程后，没有必要再继续开展工作。

II. The Future Work of the Expert Group

China welcomes the *Comprehensive Study on cybercrime* and the outcomes of all the Expert Group meetings. China appreciates the UNODC, as the Secretariat, for its great efforts spared to this process.

The UN has established the Ad Hoc Committee to negotiate the convention on countering cybercrime, for which the UNODC will serve as the Secretariat as well and provide support to Member States during this process. The negotiation process provides a valuable opportunity for Member States to further deepen cooperation on combating cybercrime. Member States should spare no effort to support and participate in the work of the Ad Hoc Committee, in order to conclude a new and global convention against cybercrime as soon as possible. Bearing in mind that the organizational session of the Ad Hoc Committee is scheduled in May 2021, and the substantive negotiations will follow, it is better not to duplicate the work on cybercrime, and it is necessary to ensure States, especially the developing countries with limited resources, and UNODC could concentrate on the work of the Ad Hoc Committee. Taking into consideration of the above, China believes that it is unnecessary for the Expert Group to continue its work after the current meeting.

COMENTARIOS DE COLOMBIA

A LA RECOPILACIÓN DE TODAS LAS CONCLUSIONES Y RECOMENDACIONES PRELIMINARES SUGERIDAS POR LOS ESTADOS MIEMBROS DURANTE LAS REUNIONES DEL GRUPO DE EXPERTOS ENCARGADO DE REALIZAR UN ESTUDIO EXHAUSTIVO SOBRE DELITO CIBERNÉTICO CELEBRADAS EN 2018, 2019 Y 2020

Ministerio de Relaciones Exteriores de Colombia
19 de marzo de 2021

Considerando la invitación de la Secretaría de las Naciones Unidas para que, de cara a la reunión del Grupo de Expertos que tendrá lugar del 6 al 8 de abril 2021 en Viena, los Estados Miembros proporcionen por escrito observaciones sobre las conclusiones y recomendaciones preliminares, así como sobre la labor futura del Grupo de Expertos (UNIEG), a continuación, nos permitimos remitir los comentarios preliminares por parte de Colombia:

Habida cuenta de la aprobación de la Resolución 74/247 de la Asamblea General de las Naciones Unidas, por medio de la cual se estableció un Comité intergubernamental especial de expertos de composición abierta para elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, se considera fundamental que, dentro de las conclusiones y recomendaciones, se insista en la importancia de que la nueva convención tenga en cuenta los marcos e instrumentos jurídicos internacionales existentes, como son la Convención de las Naciones Unidas sobre la Delincuencia Organizada Transnacional (UNTOC) y la Convención de Budapest sobre la Ciberdelincuencia, dado que la legislación y las prácticas de la mayoría de los Estados están conforme a los acuerdos existentes, por lo cual, los estándares futuros deben ser compatibles con estos.

Resaltamos la importancia de que la elaboración de la nueva convención se realice de forma inclusiva, transparente y basada en el consenso, así como se llevaron a cabo los anteriores procesos de las Naciones Unidas para concertar la Convención contra la Delincuencia Organizada Transnacional y la Convención contra la Corrupción. Esto contribuirá a prevenir futuras controversias en la materia.

Adicionalmente, se observa que no hay claridad en cuanto al contenido de la futura convención, y llama la atención que en el documento se hacen algunas referencias contradictorias al respecto. Por ejemplo, en materia de cooperación directa con las empresas o particulares prestadores de servicios de internet. Cabe resaltar que el tema de la promoción de la cooperación sólida y basada en la confianza entre los sectores público y privado en el ámbito de la ciberdelincuencia, es un tema de la mayor importancia, por lo cual resulta fundamental tener una posición consistente en el tema.

Se considera imperativo intensificar la cooperación internacional para la investigación de los delitos cibernéticos, en especial frente a la gestión de pruebas electrónicas, cadena de custodia, conservación de datos y análisis forense. La transmisión y almacenamiento de datos electrónicos es un asunto que requiere atención urgente, así como la definición de mecanismos que permitan la comunicación y respuesta rápida entre autoridades homólogas de los diferentes Estados, a través de canales apropiados.

Por otra parte, para acortar la brecha digital, igualmente se considera fundamental que las conclusiones y recomendaciones confirmen la importancia del fortalecimiento de capacidades, especialmente en lo referente a la justicia penal, y a los programas de educación y entrenamiento como una forma de prevención.

Sin embargo, el documento presenta muchas repeticiones, por lo cual se sugiere evitar la duplicación de referencias a los mismos puntos, como, por ejemplo, a la posibilidad y viabilidad de otorgar al Grupo de Expertos o a la UNODC el mandato de realizar y publicar anualmente una evaluación de las tendencias de la ciberdelincuencia; o a la necesidad de actualizar las legislaciones nacionales.

En la sección IV. Referente a la reunión del 27 al 29 de julio de 2020, en la parte A. sobre "Cooperación Internacional", numeral 8, literal b), sobre la discusión frente al nuevo tratado, se informa que: "*Se reiteró la opinión de que el Convenio sobre la ciberdelincuencia del Consejo de Europa tenía un ámbito de aplicación limitado por su condición de instrumento regional*". Sobre ese particular, se considera importante aclarar que dicha opinión fue presentada por "algunos países", y que dicho convenio actualmente tiene alcance global, por lo cual Estados de todas las regiones del mundo hacemos parte de dicho instrumento.

Llaman la atención las referencias a la necesidad de desarrollar normas sobre comportamiento responsable de los Estados en el ciberespacio, lo cual es un tema que está siendo abordado directamente en la Comisión Primera de las Naciones Unidas, y va más allá de los temas referidos al delito cibernético.

Finalmente, consideramos que se debe analizar la posibilidad de continuar con el UNIEG, en la medida en que proporciona una valiosa plataforma para compartir experiencias e identificar soluciones en materia de ciberdelito.

……

7th Meeting of the Intergovernmental Expert Group (IEG) on Cybercrime
Comments of the Czech Republic
On IEG Conclusions and Recommendations and Its Future Work

With respect to the UNODC note verbale CU 2021/108(A)/DTA/OCB/CSS the Czech Republic would like to express its deep appreciation of the long-term valuable work and beneficial outcomes of the IEG and has the honour to submit below its contribution to the topics of the 7th meeting of the IEG which shall take place from 6 to 8 April 2021.

Agenda Point 2 – Consideration of Preliminary Conclusions and Recommendations

The Czech Republic takes this opportunity to point out the following recommendations which it finds of utmost importance and relevance:

A. Legislation and frameworks

(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;

(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;

(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;

(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;

B. Criminalization

(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;

(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;

C. Law enforcement and investigations

(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;

(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;

(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;

(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.

D. Electronic evidence and criminal justice

(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;

(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;

(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;

E. International cooperation

(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.

(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;

(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;

(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;

(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;

(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;

(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;

(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;

(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;

(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;

F. Prevention

(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;

(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;

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

(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;

(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;

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

Agenda Point 3 – Discussion of Future Work of IEG

The Czech Republic highly values the work of the IEG which has provided a unique global platform for the exchange of information and practice for experts and practitioners in the area of cybercrime. The IEG has formulated a large number of crucial and significant recommendations, some of which are outlined above, and the Czech Republic is convinced a discussion forum to follow-up on the IEG recommendations is very meaningful and needed. It is clear that the most repeated recommendations include calls for capacity building and technical assistance under the auspices of the UNODC as well as further exchange of experience and best practices in the area of electronic evidence and cybercrime.

It must be noted that the role of the newly established Ad Hoc Committee is to focus on the considerations and negotiations of a potential new instrument on cybercrime and that its mandate does not include expert discussions on up-to-date cybercrime related issues and exchange of experience. On the other hand, it would be advisable if the Ad Hoc Committee drew upon the practical conclusions and expertise of the IEG in its work.

The Czech Republic therefore strongly supports the establishment of a new expert platform under the CCPCJ which would build upon the work of the IEG and provide an operative global forum for experts to discuss best practices and experience as well as the provision of capacity building and enhancing international cooperation in the area of electronic evidence and fight against cybercrime.

The Czech Republic therefore suggests the 7th meeting of the IEG should submit its conclusions and recommendations for the consideration of the 30th session of the CCPCJ to be held in May 2021 and propose the establishment of a new platform as a follow-up discussion forum to the IEG to tackle current global issues and trends related to cybercrime.

EUROPEAN UNION

Expert Group to Conduct a Comprehensive Study on Cybercrime

Vienna, 6-8 April 2021

EU comments

on the future work of the Expert Group

The European Union and its Member States re-iterate the importance of retaining a forum for experts and practitioners to exchange information and practical experience on cybercrime.

Such forum would not present any duplication with the future work of the ad hoc committee established pursuant to UNGA resolution 74/247. The ad hoc committee is mandated with the one task to "elaborate a comprehensive international convention" on cybercrime "taking into full consideration … in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime". Already the resolution clarifies that there is no competition between the work of the ad hoc committee and the existing forum for experts and practitioners. On the contrary, the first draws on the work of the latter. We should maintain such beneficial situation for the future.

While cybercrime develops and increases further, we should not deprive our practitioners of a very helpful tool allowing to compare notes, exchange experiences and best practices, identify necessary capacity building etc.

The United Nations Office on Drugs and Crime as UN hub of expertise on these matters, should facilitate the work of the forum referred to above. Also bearing in mind financial aspects, the future forum for experts and practitioners should therefore meet in Vienna.

France

Contribution pour la 7ème session du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité

Vienne, 6-8 avril 2021

En réponse à la note verbale CU 2021/108(A)/DTA/OCB/CSS et dans la perspective de la septième réunion du groupe intergouvernemental, à composition non limitée, chargé de réaliser une étude approfondie sur le problème de la cybercriminalité (IEG) qui examinera de toutes les conclusions et recommandations préliminaires issues de ses quatrième, cinquième et sixième réunions, tenues en 2018, 2019 et 2020, formulera des conclusions et recommandations à présenter à la Commission pour la prévention du crime et la justice pénale ; et débattra sur les futurs travaux du groupe d'experts,

La France a l'honneur de transmettre les observations suivantes :

I. Observations générales

La cybercriminalité constitue l'une des principales formes émergentes de criminalité aujourd'hui dans le monde, qu'elle prenne la forme d'attaques directes contre des systèmes informatiques ou de l'utilisation des moyens numériques pour faciliter la préparation ou la commission d'une infraction. En pleine recrudescence, de nombreuses attaques visent les particuliers mais aussi les entreprises et les administrations. Les hôpitaux ont été particulièrement visés par les cyber-attaques ces derniers temps, confirmant que la pandémie de Covid a également accru notre vulnérabilité : le centre hospitalier universitaire de Rouen en décembre 2019, le centre hospitalier de Dax et le centre hospitalier de Villefranche-sur-Saône (Rhône) ce mois-ci ont été victimes d'attaques par des rançons.

Par sa nature même, la cybercriminalité revêt dans la majorité des cas un caractère transnational, rendant ainsi indispensable le renforcement de la coopération internationale pour mieux partager sur l'état de la menace, prévenir et faire cesser les crimes et délits mais également poursuivre les auteurs pour lutter contre l'impunité.

Dans ce contexte, la France salue les efforts de la communauté internationale en matière d'échange de bonnes pratiques et de réflexion visant à améliorer les outils dédiés à la lutte contre cette forme de criminalité, en particulier mis en avant dans les travaux de l'IEG. Compte tenu de l'expertise développée dans ce cadre, la France est attachée au maintien d'un groupe d'experts sur la cybercriminalité, à Vienne.

La France salue également les activités d'assistance technique développées, notamment dans le cadre de Programme mondial sur la cybercriminalité de l'Office des Nations unies contre la drogue et le crime (ONUDC), d'Interpol mais également du Conseil de l'Europe et de l'Union européenne.

II. Les recommandations

La France se félicite des discussions approfondies qu'ont suscitées les travaux du groupe d'experts lors de ces dernières réunions et souligne notamment l'importance des recommandations suivantes, sans pour autant être exhaustif :

A. Législation et cadres

o) L'ONUDC devrait rechercher des synergies et coopérer étroitement avec d'autres parties prenantes ou organisations, telles que le Conseil de l'Europe et l'Organisation des États américains (OEA), dans le domaine des programmes de renforcement des capacités de lutte contre la cybercriminalité, afin que les activités et les initiatives dans ce domaine ne soient pas dispersées ou fragmentées ;

p) Les États Membres devraient continuer à utiliser le Groupe d'experts comme plateforme d'échange d'informations, et de meilleures pratiques, y compris de lois et de clauses types, sur des questions telles que la compétence, les techniques d'enquête spéciales et les preuves électroniques, y compris les défis posés par leur nature volatile et leur recevabilité devant les tribunaux, et la coopération internationale ;

t) Les États Membres devraient appliquer les instruments juridiques multilatéraux existants sur la cybercriminalité, tels que la Convention du Conseil de l'Europe sur la cybercriminalité (ou Convention de Budapest) ou y adhérer, ces instruments constituant, pour de nombreux États, des modèles de meilleures pratiques en matière de mesures à prendre face à la cybercriminalité aux niveaux national et international ;

B. Incrimination

a) Les États Membres devraient tenir compte du fait que de nombreuses dispositions de droit pénal matériel visant la criminalité « hors ligne » peuvent également s'appliquer aux infractions commises en ligne. C'est pourquoi, pour renforcer les activités de détection et de répression, les États Membres devraient appliquer les dispositions existantes de droit national et international, le cas échéant, pour combattre la criminalité dans l'environnement numérique ;

j) Les États Membres devraient adopter et mettre en œuvre des cadres juridiques nationaux permettant l'admission de preuves électroniques dans les enquêtes et les poursuites pénales, y compris le partage opportun de preuves électroniques avec les partenaires étrangers chargés de la détection et de la répression ;

o) Les États Membres devraient effectuer des recherches afin d'identifier les tendances des activités sous-jacentes à la cybercriminalité et examiner plus avant la possibilité et la faisabilité de charger le Groupe d'experts ou l'ONUDC de procéder, annuellement, à une évaluation des tendances de la cybercriminalité et d'en diffuser les résultats, avec le concours des États Membres ;

p) Les États Membres devraient envisager d'adopter des stratégies globales de lutte contre la cybercriminalité, qui comprennent la réalisation d'enquêtes de victimisation, ainsi que des activités de sensibilisation et d'autonomisation des victimes potentielles de la cybercriminalité ;

C. Détection et répression

b) Toutefois, d'autres États Membres ont fait remarquer qu'il n'était ni nécessaire ni opportun d'envisager de disposer d'un nouvel instrument juridique mondial dans la mesure où les activités de renforcement des capacités, les échanges actifs et la coopération entre les services de détection et de répression ainsi que l'application des instruments existants, tels que la Convention du Conseil de l'Europe sur la cybercriminalité (ou Convention de Budapest), étaient les meilleurs moyens de faire face aux problèmes que posait la cybercriminalité et de dispenser une formation adéquate aux enquêteurs, procureurs et juges. D'après cette proposition, les États Membres devraient continuer d'utiliser les instruments juridiques multilatéraux existants dans le domaine de la cybercriminalité, tels que la Convention de Budapest, ou y adhérer, étant donné que nombre de ces États estiment que cette convention représente l'instrument d'orientation le plus pertinent pour élaborer une législation interne appropriée – tant de procédure que de fond – et faciliter la coopération internationale en matière de lutte contre la cybercriminalité ;

f) Les États sont encouragés à continuer de confier à l'ONUDC les mandats et les ressources nécessaires afin que les projets de renforcement des capacités menés dans ce domaine débouchent sur des résultats tangibles ;

g) Les pays devraient consacrer des ressources au développement des compétences nécessaires pour enquêter sur les affaires de cybercriminalité et à la création de partenariats qui tirent parti de mécanismes de coopération afin d'obtenir des éléments de preuve essentiels ;

h) Les États Membres devraient continuer de s'efforcer de mettre en place des services, organismes et structures spécialisés dans la lutte contre la cybercriminalité au sein des services de détection et de répression, des services de poursuite et de l'appareil judiciaire, et leur fournir l'appui nécessaire en les dotant des compétences et des moyens qu'il convient pour qu'ils soient en mesure de répondre aux défis que pose la cybercriminalité et puissent obtenir, échanger et utiliser des preuves électroniques dans les procédures pénales ;

i) Pour lutter contre la cybercriminalité, il faut adopter des stratégies de détection et de répression à moyen et à long termes et coopérer avec des partenaires internationaux afin de désorganiser les marchés. Ces stratégies devraient donc être proactives et de préférence cibler les groupes cybercriminels organisés dont les membres peuvent se trouver dans différents pays ;

k) Les règles de droit procédural interne doivent rester en phase avec les avancées technologiques et faire en sorte que les services de détection et de répression soient en mesure de lutter contre la criminalité en ligne. Des lois adaptées devraient être rédigées en tenant compte des notions techniques applicables et des besoins concrets des enquêteurs chargés des affaires de cybercriminalité et dans le respect des garanties d'une procédure régulière, de la vie privée, des libertés civiles et des droits humains, ainsi que des principes de proportionnalité et de subsidiarité et des garanties en matière de contrôle judiciaire. En outre, les États Membres devraient consacrer des ressources à l'adoption d'une législation interne autorisant ce qui suit :

i) Les demandes de protection rapide des données informatiques adressées à la personne qui contrôle ces données – à savoir les fournisseurs d'accès à Internet et de services de communications

– en vue de conserver les données et de préserver leur intégrité pendant une période déterminée compte tenu de leur volatilité possible ;

ii) Les perquisitions et les saisies de données stockées sur des appareils numériques, qui constituent souvent les éléments de preuve les plus pertinents d'une infraction électronique ;

iii) Les ordonnances demandant la production de données informatiques soumises à un régime de protection de la vie privée moins rigoureux, comme les données concernant le trafic et les abonnés ;

iv) La collecte en temps réel de données relatives au trafic et de contenu lorsqu'il y a lieu ;

v) La coopération internationale entre les autorités nationales de détection et de répression ;

l) Étant donné que les enquêtes sur la cybercriminalité exigent une certaine créativité, une perspicacité technique et la coopération entre les procureurs et les services de police, les pays devraient les encourager à collaborer étroitement dès l'ouverture de l'enquête afin de réunir suffisamment de preuves pour inculper les personnes identifiées ;

o) Les pays devraient faire preuve de souplesse en ce qui concerne la détermination de la base juridictionnelle applicable aux affaires de cybercriminalité, notamment en s'appuyant davantage sur le lieu de prestation des services informatiques et non de stockage des données ;

D. <u>Preuve</u>

f) La recevabilité d'une preuve électronique ne devrait pas dépendre du fait qu'elle ait été recueillie sur le territoire national ou non, tant que sa fiabilité n'est pas compromise et qu'elle a été obtenue légalement, notamment conformément aux dispositions d'un traité d'entraide judiciaire ou d'un accord multilatéral ou en coopération avec le pays compétent, par exemple ;

g) Les États Membres devraient prendre les mesures nécessaires pour adopter une législation garantissant la recevabilité des preuves électroniques, tout en gardant à l'esprit qu'il appartient à chaque pays de se prononcer sur la recevabilité d'une preuve, y compris électronique, conformément au droit national ;

bb) Les États sont encouragés à communiquer entre eux pour améliorer encore l'assistance judiciaire et la coopération en matière de répression au niveau international en optimisant les procédures et méthodes pertinentes afin de faciliter la conduite des enquêtes et la collecte de preuves ;

E. <u>Coopération internationale</u>

b) En ce qui concerne les mécanismes de coopération internationale, les États sont encouragés à adhérer aux traités multilatéraux existants, tels que la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention sur la cybercriminalité du Conseil de l'Europe, qui constituent le fondement juridique de l'entraide judiciaire, ou à s'y référer, en l'absence d'un traité bilatéral d'entraide judiciaire. En l'absence de tout traité, les États peuvent demander à un autre État de coopérer sur la base du principe de réciprocité ; la Convention du Conseil de l'Europe sur la cybercriminalité devrait également être utilisée comme référence pour les activités de renforcement des capacités et d'assistance technique dans le monde entier, et l'attention a été appelée sur les négociations en cours concernant le deuxième protocole additionnel visant à

renforcer encore la coopération transfrontalière. L'avis a été réitéré que la Convention du Conseil de l'Europe sur la cybercriminalité n'avait qu'une application limitée compte tenu de son caractère régional, de l'état des ratifications, de l'absence de démarche globale, de la non-prise compte des tendances actuelles en matière de cybercriminalité et du fait qu'elle ne convenait pas pleinement aux pays en développement. L'attention a été appelée sur la résolution 74/247 de l'Assemblée générale, dans laquelle l'Assemblée avait décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Un certain nombre de délégations ont estimé que l'élaboration d'une convention des Nations Unies améliorerait l'efficacité de la coopération internationale dans le domaine de la lutte contre la cybercriminalité. D'autres délégations ont fait valoir qu'il ne faudrait pas que les nouveaux cadres ou instruments sur la cybercriminalité aillent à l'encontre des cadres ou instruments existants et que les États soient amenés à abandonner les traités actuels ou les engagements pris précédemment, ainsi que les accords déjà en place, ou à ne pas s'y conformer ;

t) Les pays sont invités à rejoindre les réseaux autorisés de praticiens pour conserver et échanger des preuves électroniques recevables, à les utiliser plus largement et à les renforcer, y compris les réseaux 24/7, les réseaux spécialisés dans la cybercriminalité et les canaux d'INTERPOL pour une coopération policière rapide, ainsi qu'à mettre en place des réseaux avec des partenaires stratégiquement alignés, en vue de partager des données sur les questions de cybercriminalité, d'intervenir rapidement et de réduire au minimum la perte de preuves essentielles. Il a en outre été recommandé de recourir à la coopération policière et à d'autres méthodes de coopération informelle avant d'utiliser les canaux d'entraide judiciaire ;

u) Chaque État doit désigner un véritable point de contact joignable 24 heures sur 24, sept jours sur sept, doté de ressources suffisantes, pour faciliter la conservation des données numériques ainsi que le traitement des demandes traditionnelles d'entraide judiciaire internationale en matière pénale, en s'inspirant du dispositif efficace de gel des données prévu par la Convention du Conseil de l'Europe sur la cybercriminalité ;

rr) La Commission pour la prévention du crime et la justice pénale devrait envisager de prolonger le plan de travail du Groupe d'experts au-delà de 2021 en tant que forum permettant aux praticiens d'échanger des informations sur la cybercriminalité ;

tt) Il a été recommandé que l'élaboration de toute nouvelle convention soit gérée par les experts de l'ONUDC à Vienne ;

uu) Certains intervenants ont recommandé que la Commission pour la prévention du crime et la justice pénale renouvelle le mandat du Groupe d'experts et convienne d'un plan de travail au-delà de 2021, qui devrait également prendre en compte les nouvelles formes de cybercriminalité et l'examen des questions liées à l'exploitation et aux atteintes sexuelles visant les enfants en ligne ;

xx) Dans leurs interventions, les représentants de nombreux États Membres ont salué l'adoption de la résolution 74/247 de l'Assemblée générale. Il a été déclaré que l'élaboration de la nouvelle convention, conformément à cette résolution, devrait être inclusive, transparente et fondée sur le consensus, et que les travaux antérieurs des Nations Unies relatifs à l'élaboration de la Convention

contre la criminalité organisée et la Convention contre la corruption pourraient servir d'exemple dans ce sens ;

aaa) La communauté internationale devrait donner la priorité au renforcement des capacités et à d'autres formes d'assistance destinée à améliorer la capacité des autorités nationales à lutter contre la cybercriminalité, en particulier contre l'exploitation sexuelle et les atteintes sexuelles visant des enfants en ligne ;

F. <u>Prévention</u>

d) Les activités de sensibilisation à la cybersécurité devraient figurer dans le programme de l'enseignement primaire, secondaire et supérieur, et s'adresser tant aux étudiants qu'aux enseignants. Idéalement, elles devraient faire partie intégrante des stratégies nationales sur la cybersécurité. Les États devraient par ailleurs mettre en commun leurs expériences sur la manière d'utiliser ces stratégies pour prévenir la cybercriminalité. Ils devraient en outre accorder une attention particulière mesures préventives destinées aux jeunes, y compris aux primo-délinquants, afin de prévenir la récidive ;

k) Les États devraient renforcer les stratégies visant à lutter contre le recours, par les groupes criminels traditionnels, à des cyberoutils pour dissimuler leurs communications et leurs activités ;

s) Les droits humains fondamentaux et les libertés fondamentales doivent être protégés partout, y compris dans le domaine numérique et le cyberespace, sans considération de frontières et sans aucune interférence ou restriction.

III. Les futurs travaux du Groupe d'expert

La recrudescence de la cybercriminalité de ces dernières années illustre la nécessité de conserver un forum permettant aux experts et aux praticiens de mettre en commun leur expertise collective en la matière.

La France est convaincue du rôle central de la Commission pour la prévention du crime et la justice pénale (CCPCJ) et du Groupe intergouvernemental d'experts sur la cybercriminalité (IEG) pour faciliter et renforcer la coopération internationale en matière de lutte contre la cybercriminalité.

En dépit de l'impossibilité de parvenir à un accord sur l'ébauche d'étude présentée par le secrétariat en 2013, la France considère que l'IEG a permis à des experts du monde entier de pouvoir échanger des informations utiles et des bonnes pratiques en matière de lutte contre la cybercriminalité. Les discussions au sein de l'IEG ont ainsi inspiré un certain nombre d'Etats à réformer leur législation et renforcer leurs capacités d'action en la matière.

Elle est donc favorable à une évolution du mandat de l'IEG afin qu'il se concentre sur sa fonction de forum unique au sein des Nations Unies pour que les experts puissent se réunir et échanger sur la cybercriminalité, à Vienne. L'ONUDC, en tant que secrétariat de la CCPCJ, est en effet la seule entité de l'ONU qui dispose à la fois du mandat et de l'expertise pour faciliter ces échanges.

La France souhaite souligner que les futurs travaux de l'IEG ne doivent pas se dupliquer pas avec ceux à caractère normatif qui seront menés dans le cadre du comité ad hoc établi par la résolution 74/247 de l'Assemblée générale des Nations unies, dont le mandat se limite à la négociation d'une convention internationale et qui ne permet pas aux experts d'échanger de manière opérationnelle.

Comments of the Islamic Republic of Iran on the topics of the seventh meeting of the Expert Group

With reference to the communication, dated 5 March 2021, regarding comments and recommendations relating to the topics of the seventh meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, which will be held in Vienna, Austria, from 6 to 8 April 2021, I wish to transmit to you herewith the following comments and proposals of the Islamic Republic of Iran on the preliminary conclusions and recommendations:

1. As underlined in the Draft Report, the preliminary recommendations and conclusions contained therein do not imply endorsement by the Expert Group rather they are compilation of the views of Member States. As a result, certain recommendations or conclusions are contradictory and also do not reflect positions of many Member States. Therefore, it is necessary that the Report of the Expert Group be consensually-agreed-upon and that it accommodate views and considerations of all Member States, otherwise, the Draft Report may not be endorsed and supported by all Member States.
2. Regarding the definition and criminalization of cybercrime acts, it should be noted that the relevant applicable international legal frameworks as well as the practice of the United Nations and Member States distinguish between crimes committed for material purposes (such as transnational organized crime) and those perpetrated for political purposes (such as terrorism). The very fact that terrorism, in contrast with transnational organized crime, constitutes a threat to the international security more telling on such

divergence and differences. In this respect, we are of the view that it is of practical utility to differentiate between cybercrimes and use of cyberspace by terrorists for commission of terrorist acts. In this regard, given the technical nature of the Expert Group and its mandates on "cybercrime", the recommendations and conclusions of the Expert Group should only address crimes committed for material purposes which will reflects the very notion of cybercrime.

3. As regard the references made in the Draft Report to the Budapest Convention, it is essential to take into account that quite diversified views exist among Member States regarding the Budapest Convention. The Convention is a regional instrument and many Member States were not involved in its negotiations a fortiori it has not identified and established a common ground among all legal systems and therefore does not accommodate the various needs and views of Member States. By the same token, the Budapest Convention could not be used as a standard for capacity-building and technical assistance worldwide considering in addition that the Convention as a European Convention could not have taken into account the differences among Member States' legal and political systems. As such, the Expert Group may not recommend all Member States to join or use the Convention for international cooperation; any recommendation or conclusion on this would not be endorsed by all Member States and would be at variance with the differences that exist among Member States on the Convention.
4. Regarding the UNTOC and references in the Draft Report concerning its possible utility as a legal basis for international cooperation in fighting, it should be stressed that there exist no consensus on whether the Convention could be applied on cybercrime cases or not. Moreover, after the negotiations and adoption the UNTOC, the world has witnessed transformative changes in the crimes committed in and via cyberspace and the *modi operandi* of criminals has exponentially diversified. The UNTOC which has been adopted decades ago could hardly meet the specific and emerging forms of cybercrime. To effectively fighting against cybercrime a

resilient and up-to-date international legal framework, one that efficiently responds the emerging forms of cybercrime is of utmost importance.

5. International cooperation in combating cybercrime requires a sound and efficient international legal framework. While such cooperation should also be with due respect to domestic laws, the international legal framework should remain the primary basis for cooperation so as to ensure harmonization needed for smooth cooperation at the international level.
6. As regards the handling of electronic evidence and their admissibility, the IEG may not prescribe the need for reforming national legislations since legal systems are diversified and it is they very prerogative of States to determine such matters. The IEG may only recommend States to take into account best practices as examples for reforming their where appropriate and where they deem necessary as so.

Best Regards,

Nabi Azami,

Minister Counselor,
Permanent Mission of the I.R.Iran to the United Nations and other International Organizations in Vienna.

Comments by the Government of Japan for the 7th IEG meeting

March 19, 2021

With regard to the production of conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice, Japan supports the adoption of the following conclusions and recommendations, which are of particular importance for combating cybercrime.

1 Legislation and frameworks

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.

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.

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.

2 Criminalization

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.

3 Law enforcement and investigations

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.

Countries should devote resources to developing expertise to investigate cybercrime and to creating partnerships that employ cooperation mechanisms to obtain vital evidence.

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.

4 Electronic evidence and criminal justice

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.

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.

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.

5 International cooperation

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.

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.

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.

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.

6 Prevention

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

Ministerie van Justitie en Veiligheid

UNODC / IEG Study on Cybercrime

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding "2DRC"

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
E.J.H. Planken

T 070 370 79 11

Datum
17 maart 2021

Ons kenmerk
3258760

memo

The Netherlands expert input for comments in view of the 7th IEG cybercrime meeting in Vienna from 6 to 8 April 2021

In the note verbale of 5 March 2021 (CU 2021/108(A)/DTA/OCB/CSS) the secretariat of the UNODC invites participating countries in the IEG cybercrime to provide comments and recommendations relating to the topics of the seventh meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, which will be held in Vienna, Austria, from 6 to 8 April 2021. In response, the Netherlands expert delegation wishes to draw attention to the following points.

Agenda item 2: *Consideration of all preliminary conclusions and recommendations resulting from the fourth, fifth and sixth meetings of the Expert Group, held in 2018, 2019 and 2020, and production of conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice*

The past three meetings of the IEG have resulted in an impressive list of 206 conclusions and recommendations. Condensing this into a short consolidated list may disregard the fruits of broad discussions with inputs based on many varied good practices and insights. On the other hand a short and consolidated list may be more effective in steering the future developments in the pursuit of a global effective approach to the criminal justice problems caused by cybercrime and the use of electronic evidence as a result of the ever growing digitalisation of societies worldwide.

When studying the 206 conclusions and recommendations, a picture emerges of some more overarching ones, on which member states in the discussions seem to be able to find consensus. In this respect the Netherlands expert delegation recommends to include the following in the consolidated list to be submitted to the CCPCJ.

- ***National legislation and frameworks are necessary conditions for effectively addressing cybercrime***
    - Member States should adopt and apply domestic legislation to criminalize cybercrime conduct and to grant law enforcement authorities procedural authority to investigate alleged crimes.
    - Member States' national legislation and frameworks should provide for possibilities to 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.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
"2DRC"

Datum
17 maart 2021

Ons kenmerk
3258760

- Legislative provisions have to withstand the test of time with regard to future developments in technology by using technologically neutral formulations.
- In formulating policies and legislation, Member States should consider the need to strike a proportionate balance between human rights protection on the one hand, and national security, public order, respect for the sovereignty of States and the legitimate rights of third persons on the other. Policies and legislation should not only cover enforcement measures against illegal conduct, but also focus on crime prevention and provide help to victims of crime and assistance to the general public.
- 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. Member States should take into account that many existing substantive criminal law provisions designed for "offline" crime may also be applicable to crimes committed online.
- Cybersecurity practices are distinct from efforts to combat cybercrime. States should develop both a national cybercrime policy and legislation and a national cybersecurity policy.
- Member States should develop and implement national 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.
- 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.
- To ensure that relevant issues are properly considered, Member States should consult all relevant stakeholders, including intergovernmental stakeholders, the private sector and civil society. 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.

- **Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by adequate capacity and capabilities for law enforcement, prosecution and adjudication**
  - 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. States should 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 are to be

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
"2DRC"

Datum
17 maart 2021

Ons kenmerk
3258760

taken into account. Member States should develop a network of focal points between law enforcement agencies, judicial authorities and prosecutors.
- 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.
- 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.
- Member States should 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.
- 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 obtain and preserve evidence in a reliable manner.

- **States should engage actively in capacity-building for all Member States in need of assistance, in particular developing countries**
  - Such capacity-building activities and technical assistance should be politically neutral and free from undue 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.
  - 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.
  - UNODC should seek synergies and cooperate closely with regional organizations such as OAS, the Council of Europe and other stakeholders such as the Global Forum on Cyber Expertise, to ensure that activities and initiatives in these area are not dispersed or fragmented.
  - Member 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 the areas mentioned above.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
"2DRC"

Datum
17 maart 2021

Ons kenmerk
3258760

- **International cooperation between Member States is vital to an effective approach on cybercrime as well as to prevent safe havens for criminals**
    - Effective international cooperation requires national laws that create procedures enabling international cooperation. Thus, national laws must allow for international cooperation among law enforcement agencies.
    - Beyond domestic laws, international cooperation on cybercrime relies on both formal, treaty-based cooperation and traditional police-to-police assistance.
    - 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.
    - 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.
    - Member States should build on tried-and-tested existing international instruments to which they are encouraged to accede where possible, or, in the absence of a bilateral mutual legal assistance treaty, to use existing multilateral treaties such as the United Nations Convention against Transnational Organized Crime.
    - Member States should engage in the process of the General Assembly resolution 74/247, in which the Assembly has 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. The Netherlands reiterates 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.

Agenda item 3: *Discussion of future work of the Expert Group*

In the experience of the Netherlands experts, the role and impetus of this UN IEG Cybercrime has grown over the years, especially when implementing the 2018-2021 work plan. The format provided insights in, as well as debates on, good practice, new ideas and working methods to prevent and combat cybercrime from all over the world. As is demonstrated by, inter alia, the increase of activities of the C-PROC office in Bucharest, this consequently led to a considerable increase in capacity building on cybercrime and electronic evidence worldwide.

The expert delegation of the Netherlands would therefore recommend the following regarding the future work of the IEG:

- The IEG or a similar entity replacing it should continue to provide a forum for exchange of information among practitioners and experts on national

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
"2DRC"

Datum
17 maart 2021

Ons kenmerk
3258760

legislation, best practices, technical assistance and international cooperation. Such exchange includes 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.

- This work should be complementary to that of the Ad Hoc Committee pursuant to General Assembly resolution 74/247 since:
  - it is not part of the AHC's mandate under that resolution;
  - it does not include the elaboration of a comprehensive international convention on cybercrime, which is the exclusive mandate of the Ad Hoc Committee.
- The venue of the IEG or entity replacing it should be Vienna, being the expertise and knowledge-based UN headquarters for this topic, where this theme has so far been tackled with UNODC as Secretariat for the IEG and implementing the Global Programme on Cybercrime.
- Member States should evaluate the possibility and feasibility of mandating the Expert Group or entity replacing it to conduct and make available on a regular basis, on the basis of substantive contributions by Member States, an assessment of cybercrime trends and new threats.

OBSERVACIONES DEL ESTADO DE NICARAGUA SOBRE RECOPILACIÓN DE CONCLUSIONES Y RECOMENDACIONES PRELIMINARES SUGERIDAS POR LOS ESTADO MIEMBROS DE UNODC RELATIVAS A DELITOS CIBERNÉTICOS

INTRODUCCIÓN

El Gobierno de Nicaragua, atendiendo la Nota de referencia CU 2021/108(A)/DTA/OCB/CSS, del 5 de marzo 2021, emitida por la Secretaria de las Naciones Unidas, en la cual se invita a los Estados Miembros a formular observaciones y recomendaciones al documento elaborado por el Grupo de Expertos de la Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC), denominado *"Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético celebrada en 2018, 2019 y 2020"*, comparte las siguientes observaciones y recomendaciones:

A. LEGISLACIÓN Y MARCOS

1- Los Estados Miembros deberían formular legislaciones o leyes tecnológicamente neutrales, tomando en cuenta el rápido avance

de la tecnología para garantizar la permanencia y aplicabilidad en el tiempo.

2- Los Estados Miembros deberían respetar los derechos soberanos de los otros Estados, en cuanto a la formulación de políticas y leyes que estén estrictamente de acuerdo con sus circunstancias y necesidades nacionales para enfrentar la ciberdelincuencia.

3- La cooperación de todos los Estados es fundamental para enfrentar la ciberdelincuencia. Esta cooperación debería al menos abarcar la investigación, recopilación de pruebas, los enjuiciamientos, el fallo y en algunos casos eliminación de contenidos ilícitos de internet, sustentando la misma en diversas bases jurídicas entre ellas la reciprocidad, tratados bilaterales o multilaterales y otros acuerdos.

4- En las leyes que los Estados Miembros promulguen sobre el tema, se debe de procurar el equilibrio entre los Derechos Humanos, Seguridad Soberana Nacional y Seguridad Ciudadana.

5- Los Estados miembros deben de promover y desarrollar la capacitación de sus operadores de justicia (por ejemplo: policía, fiscales, jueces) sobre la ciberdelincuencia para garantizar una correcta aplicación de las leyes que se dicten sobre esta materia. Asimismo estas capacitaciones se deben de promover en alianza y coordinación con la

UNODC, que garantice las herramientas necesarias para el fomento de las capacidades tecnológicas en los Estados Miembros, sin imponer condiciones de ningún tipo, respetando el derecho soberano de los Estados.

6- Se considera como una buena práctica que los Estados Miembros observen y utilicen como un marco de referencia, las disposiciones de los instrumentos jurídicos internacionales vigentes sobre esta materia, incorporándolas en su legislación interna en la medida de lo posible, de acuerdo a sus necesidades y realidad de país.

B. TIPIFICACIÓN

7- Los Estados Miembros deberían de aprobar leyes nacionales para tipificar y sancionar de manera específica los delitos cibernéticos sin desvincularlos del Derecho Penal General.

8- La tipificación de los delitos cibernéticos debería, en la medida de lo posible armonizarse internacionalmente, en cuanto a la denominación del tipo penal y la conducta típica, sin menoscabo de la soberanía y autodeterminación de los Estados Miembros.

9- Los Estados Miembros deberían de adoptar medidas encaminadas a la prevención de la ciberdelincuencia que incluya medidas para el uso responsable del internet y las TIC en general, especialmente por parte de la niñez y adolescencia.

C. APLICACIÓN DE LA LEY E INVESTIGACIÓN

10- Los Estados Miembros deberían esforzarse para crear y reforzar unidades especializadas en ciberdelincuencia, dotándolos de los conocimientos y equipos necesarios para la prevención, investigación, persecución y sanción de ciberdelitos.

11- Los Estados miembros deberían de promulgar leyes nacionales encaminadas a la conservación rápida de datos informáticos por parte de los Proveedores de Servicios de Internet y Comunicaciones, así como garantizar la cadena de custodia de los dispositivos y datos contenidos en ellos, que sirvan como evidencia y prueba para el esclarecimiento de los delitos.

12- La legislación nacional que emitan los Estados Miembros sobre ciberdelincuencia, debería incorporar disposiciones pertinentes a las obligaciones de parte de los Proveedores de Servicios de Internet y Comunicaciones, para garantizar su cooperación en la aplicación de la Ley.

D. PRUEBAS ELECTRÓNICAS Y JUSTICIA PENAL

13- Nicaragua considera apropiado que las legislaciones internas de los Estados Miembros establezcan los datos que puedan constituir

pruebas electrónicas o digitales, por ejemplo datos de tráfico, ficheros de registro de conexión a internet, correos electrónicos, datos de abonados, información de registro de los usuarios entre otros que se almacenen, procesen o trasmitan en formato digital y que se generen durante la comisión de un ciberdelito.

E. COOPERACIÓN INTERNACIONAL

14- La Cooperación Internacional entre los Estados Miembros en materia de ciberdelincuencia, debería de tener como base jurídica la reciprocidad, estableciendo mecanismos de respuesta rápida, así como canales de comunicación entre las Autoridades Nacionales mediante oficiales enlace u otro medio efectivo y seguro para el cambio de información y pruebas electrónicas.

15- Los Estados Miembros deberían de abstenerse de aplicar medidas unilaterales ilícitas que afecten los principios de soberanía y el principio de no intervención en asuntos internos de otros Estados.

F. PREVENCIÓN

16- Los Estados Miembros deberían considerar que en sus sistemas educativos primarios y secundarios se incorpore una asignatura relativa a la Ciberseguridad y uso responsable de las TIC, a fin de prevenir la comisión de ciberdelitos y evitar ser víctimas de estos.

17- La legislación de los Estados Miembros, en materia de ciberdelincuencia, deberían procurar la prevención, investigación y sanción de la violencia de género, en particular la violencia contra las mujeres, niños y adolescentes y los delitos de odio motivados por raza, creencia religiosa y políticas, entre otros.

18- Los Estados Miembros deberían elaborar y promover Estrategias de Ciberseguridad como parte de su política interna para la prevención de la ciberdelincuencia.

19- Los Estados Miembros deberían integrar o reforzar medidas nacionales y regionales destinadas a prevenir la propagación del discurso de odio, el extremismo violento y racismo, a trávez del uso de las TIC.

G. REFERENCIAS DE NORMAS JURÍDICAS DE NICARAGUA EN MATERIA DE CIBERSEGURIDAD Y CIBERLITOS

- Decreto A.N. No. 8651 de aprobación del **"Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia"**, publicado en La Gaceta Diario Oficial No. 42 del 3 de marzo del 2020.

- Decreto Presidencial No. 24-2020 de aprobación de la **"Estrategia Nacional de Ciberseguridad 2020-2025"**, publicado en La Gaceta Diario Oficial No. 178 del 29 de septiembre del 2020.

- Ley No. 1042, **"Ley Especial de Ciberdelitos"**, publicada en La Gaceta Diario Oficial No. 201 del 30 de octubre del 2020.

- Acuerdo Administrativo No. 01-2021 de aprobación de la "**Normativa para la preservación de datos e información"**, publicada en La Gaceta Diario Oficial No. 20 del 29 de enero del 2021.

Managua, 11 de marzo, 2021

---Última línea---

Comments on Preliminary Conclusions and Recommendations of the Intergovernmental Expert Group (IEG) on Cybercrime

The seventh meeting of the UNODC Expert Group to Conduct a Comprehensive Study on Cybercrime (IEG) is scheduled to be held in Vienna, Austria, April 6 to 8 2021. In a note verbale of 5 March 2021 (CU 2021/108(A)/DTA/OCB/CSS) the UNODC secretariat invites participating countries in the IEG on cybercrime to comment and give recommendations connected to the topics of this meeting. Please find the comments from Norway below.

Re Agenda item 2:
Consideration of all preliminary conclusions and recommendations resulting from the fourth, fifth and sixth meetings of the Expert Group, held in 2018, 2019 and 2020, and production of conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice

The IEG process has resulted in a list of more than 200 conclusions and recommendations. A number of these are related and/or interconnected. Norway believes it would be useful and possible to condense this list. As a suggestion for a possible revised list to be sent to the CCPCJ, we would suggest to include the following main points:

a) National legislation (material and procedural), frameworks, "Soft law" and best practices as a foundation to uncover, prevent, combat and reduce cybercrime.

b) The importance of sufficient capacity and competence for national authorities working to counter cybercrime and work with electronic evidence in criminal cases.

c) International cooperation to counter cybercrime, and to build frameworks to support and facilitate this work.

d) Capacity building, in particular for developing countries and institutions in developing countries.

e) International cooperation between countries, in individual criminal cases as well as to prevent cybercrime

f) Support national and international research and analysis to uncover, prevent, combat and reduce cybercrime.

g) Always take into consideration the value and importance of open and interconnected internet services, data protection, privacy and public trust.

h) It is important that human rights such as freedom of expression, freedom of assembly and freedom of religion enjoy the same protection in cyberspace as elsewhere.

i) Regarding non-UN instruments: Norway is a member of the Council of Europe Convention on Cybercrime (the Budapest Convention) and the Council of Europe Convention 108 on data protection. We believe that possible future UN instruments and/or recommendations, could and should be developed in a way that does not raise issues regarding current international commitments.

Re agenda item 3:
Discussion of future work of the Expert Group

Serious cybercrime threats such as online sexual child abuse, terrorist online content, and ransomware attacks are among the challenges we have to counter efficiently and ensure rule of law. Norway considers that the UN IEG has provided a valuable forum for exchange of views, experiences and best practices. We would like to emphasize that the IEG format has provided for a forum where expertise and experience has been the focal point. We believe that this has been valuable also for the UNODC work on capacity building in the cybercrime area.

Norway would recommend that the IEG or a similar entity should continue as a forum for experts/practitioners, and that the future venue should be Vienna, with the UNODC as the secretariat.

PERMANENT MISSION OF PORTUGAL
VIENNA

PORTUGAL

Comments and Recommendations on the Future Work of the Intergovernmental Expert Group (IEG) on Cybercrime

Portugal considers that the work of the Intergovernmental Expert Group (IEG) has clearly highlighted the importance and relevance of the existence of a forum where experts and practitioners can regularly meet to exchange information, also on national legislation, best practices and experiences. These exchanges provide invaluable insights and help to foster capacity-building and technical assistance on cybercrime, while also permitting to identify trends and to signal possible new threats.

Thus, Portugal strongly reiterates the importance of retaining a forum or platform for experts and practitioners to exchange information and practical experience on cybercrime. This forum, working under the Commission on Crime Prevention and Criminal Justice (CCPCJ), should be practitioner-oriented, convening in Vienna with discussions being facilitated by the United Nations Office on Drugs and Crime (UNODC), the UN-system repository of knowledge on the matter and where the expertise and mandate in this regard lies.

Such a forum or platform would not present any duplication or overlap with the future work of the Ad Hoc Committee (AHC) established by UNGA resolution 74/247, which has a clearly defined mandate: the elaboration of a new international instrument on cybercrime, a process in which Portugal is also constructively engaging.

This practitioner-oriented forum would clearly distinguish itself from the Ad Hoc Committee (AHC) established by UNGA resolution 74/247, as it would not have a mandate for the development of any new international instrument or mechanism.

No. 25800/2021/2021/17.03.2021

ROMANIA – Reference CU 2021/108 (A) DTA/OCB/CSS

Comments on the preliminary conclusions and recommendations for the Expert Group (UNIEG)

Sharing the view of many Member States, Romania would like to underline the value of the UNIEG that has been serving as a platform for practitioners to share experience and identify solutions. The massive increase in COVID-19 related cybercrime underlines the relevance of effective measures against cybercrime, and why this Expert Group is needed now more than ever as a forum for dialogue and common responses to this challenge.
Therefore, consideration should be given to continuing the UNIEG or a similar platform should also be available in the future.

The conclusions and recommendations confirm broad agreement on capacity building to address the needs of criminal justice practitioners. This had already been one of the conclusions of the 2nd meeting of the UNIEG in 2013. **The UNIEG had major impact and led to a considerable increase in capacity building programmes on cybercrime and electronic evidence worldwide.**
The Cybercrime Programme Office of the Council of Europe was established in Romania as a consequence of the 2nd UNIEG meeting. Operational since April 2014, C-PROC is dedicated to global capacity building and by early 2021 was managing a budget of some EUR 40 million. **A continuation of the UNIEG may help promote further capacity building efforts**.

Many of the conclusions and recommendations encourage the use of existing instruments, such as the UN Convention on Transnational Organised Crime (UNTOC) or the Convention on Cybercrime. Given that the legislation and practices of most States worldwide have been shaped or influenced by existing agreements, **future standards need to be compatible with existing instruments**.

While some conclusions and recommendations suggest **a need for new international instrument** there is **no consensus on this matter within the UNIEG**. Conclusions or recommendations regarding the **possible substance and added value of new treaty are few or contradictory**. This absence of consensus on a new treaty carries the risk that the further treaty process leads to **further divisions and polarisation**.

It is essential that the upcoming UN treaty process through the Ad-Hoc Committee following the UNGA Resolution 74/247 of December 2019 to:

- be governed by decision-making by consensus;
- bring in subject-matter expertise to meet the needs of criminal justice practitioners, and should therefore be based at the UN in Vienna;
- ensure compatibility with existing instruments – including the Convention on Cybercrime – as well as meet human rights and rule of law requirements.

Serious concerns persist and must be considered in relation to the following aspects:

- International divisions. The vote on the UNGA Resolution illustrates the lack of consensus on the need and feasibility of a new treaty, which has been confirmed in all UNIEG meetings since 2011. The treaty process may thus lead to further polarization between States committed to a free and open Internet and those prepared to bring the Internet under (inter-)governmental control.
- Disruption of reforms underway or questioning legislation already adopted in some 90% of States worldwide. Romania has been contributing for many years to the efforts of international community to assist states worldwide in this process.
- Unclear scope of a future treaty with some suggesting a mix of criminal justice and national/international security. Concerns have also been raised that a new treaty would be aimed at controlling content and free speech as well as access to services on the Internet, and at placing service providers under strict governmental control.
- Concern of lower standards and of a greater digital divide. Considering diverging views on the need for and potential scope of a new treaty, and difficulties of reaching international agreement on any matter concerning cyberspace, a new treaty – if it were to be negotiated – would in all likelihood be basic in scope and depth. It would *de facto* establish a lower standard for developing countries, and thus further enhance the digital – and economic – divide, which ultimately undermines global objectives to counter serious crime on the Internet by preventing effective international crime cooperation.

Within the United Nations matters related to criminal justice are dealt with in Vienna, that is, with the UN Commission for Crime Prevention and Criminal Justice and expert groups such as the Intergovernmental Expert Group on Cybercrime. This expertise is indispensable for the preparation of the future treaty.

The future treaty needs to be based on **broadest possible consensus**. The consensus principle that applies to criminal justice matters within the UN in Vienna should thus also apply to the treaty negotiations. This is to prevent further international divisions on this matter.

Observaciones de España para la Séptima reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético.

Viena (Austria) / Online del 6 al 8 de abril de 2021

A. **Observaciones sobre las conclusiones y recomendaciones preliminares adoptadas en las reuniones anteriores del Grupo de Expertos**.

Las conclusiones y recomendaciones reflejan un amplio consenso sobre las necesidades de los actores implicados y cómo el Grupo Intergubernamental de Expertos en Ciberdelincuencia (UNIEG) ha permitido desarrollar programas de capacitación en ciberdelincuencia y prueba electrónica en todo el mundo.

En relación a la cooperación internacional, con frecuencia se recomienda acudir, en defecto de un acuerdo de cooperación bilateral, a los instrumentos multilaterales existentes, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC) o el Convenio de Budapest sobre la Ciberdelincuencia.

Aunque algunas conclusiones y recomendaciones sugieren la necesidad de un nuevo instrumento internacional -con referencia a la Resolución 74/247 de la AGNU-, no hay consenso sobre esta cuestión en el seno del UNIEG. Las conclusiones o recomendaciones sobre el posible contenido y valor añadido de un nuevo tratado son escasas o contradictorias, lo que podría conducir a divisiones en un futuro proceso de redacción.

En cualquier caso, y en relación con esta cuestión, se considera que **el procedimiento** a seguir en relación con la Resolución 74/247 de la AGNU:

- debe aportar conocimientos especializados para satisfacer las necesidades de los profesionales de la justicia penal, por lo que debería tener su sede en la sede de la ONU en Viena, esto es, en la Comisión de las Naciones Unidas para la Prevención del Delito y la Justicia Penal; a su vez, debe contar con los expertos, como los integrantes del Grupo Intergubernamental de Expertos en Ciberdelincuencia.

- debe estar regido por un sistema de toma de decisiones por consenso (principio que se aplica a los asuntos de justicia penal en la ONU en Viena); de este modo, se evitarán más divisiones internacionales en esta materia.

Y que, el **texto del futuro tratado** derivado de la Resolución 74/247 de la AGNU:

- debe ser no solo compatible con los tratados ya existentes sino también inspirado en los mismos (en particular, en el Convenio de Budapest y los conceptos que se fijan en el mismo), dado que la legislación y la práctica de la mayoría de los Estados de todo el mundo han sido moldeadas o influenciadas por ellos.

- debe cumplir con las exigencias en materia de Derechos Humanos y Estado de Derecho; esto es, sólo debe sancionar como delito las conductas específicamente tipificadas por la ley en las que la respuesta penal sea estrictamente necesaria y proporcionada en una sociedad democrática; a su vez, los poderes procesales para

investigar y asegurar las pruebas electrónicas, así como las transferencias internacionales de datos, deben estar limitados por condiciones y garantías.

B. **Observaciones y recomendaciones sobre la labor futura del Grupo de Expertos**.

El Grupo de Expertos ha proporcionado una excelente plataforma y oportunidad para que los distintos actores implicados pudieran reunirse y debatir sobre cuestiones prácticas relacionadas con la ciberdelincuencia y las pruebas electrónicas.

La expansión de la ciberdelincuencia es incesante. Por una parte, desde un punto de vista cuantitativo, paralela al incremento del uso de la red que, precisamente, ha aumentado exponencialmente a causa de la pandemia.

Por otra parte, el desarrollo tecnológico ha generado nuevas formas de lesión a bienes jurídicos merecedores de protección penal; la necesidad de tipificación de estas figuras y la importancia de una regulación lo más homogénea posible de las mismas merecen ser objeto de debate entre los prácticos.

Todo ello hace hoy más necesaria que nunca la continuidad del trabajo de este Grupo.

United States of America

Comments on Future Work of the
Intergovernmental Expert Group (IEG) on Cybercrime

The United States remains firm in its view that the Commission on Crime Prevention and Criminal Justice (CCPCJ) should extend the mandate of the Intergovernmental Expert Group on Cybercrime (IEG) beyond 2021 in order to retain a forum for experts and practitioners to exchange information and practical experience on cybercrime.

Never has there been a greater need for Member States to pool their collective expertise on cybercrime. Our prosecutors and other practitioners are not treaty negotiators; they value the IEG for the role it plays in bringing together experts who would not otherwise be able to make the connection. Withdrawing within our own borders only enables cybercriminals.

The threats we all face from cybercrime will not take a pause while diplomats in New York and Vienna direct their attention to cybercrime treaty negotiations in the Ad Hoc Committee for the next several years. We need a space where practitioners can discuss real issues free from the political debate over a new treaty.

Though the Ad Hoc Committee must draw upon practitioner expertise, including the recommendations of this IEG, it is not an expert-driven forum. It has a single mandate: to elaborate a new convention on cybercrime. Treaty negotiations are not the same as policy and practice, and we mix them at our peril.

Whether we extend the IEG or continue bringing experts together in a new format, the CCPCJ should guide its work. Future such meetings should take place in Vienna with the experts of the UN Office on Drugs and Crime (UNODC) facilitating. UNODC is the only UN entity with both the mandate and the expertise to facilitate this expert exchange, just as the CCPCJ holds the mandate to oversee crime issues in the UN system.

United States of America

Comments on Preliminary Conclusions and Recommendations of the Intergovernmental Expert Group (IEG) on Cybercrime

The Permanent Mission of the United States of America is pleased to respond to note verbale CU 2021/108(A)/DTA/OCB/CSS regarding the 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, and to provide written comments on that topic, as well as the future work of the Expert Group, for the production of conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice. The United States commends the robust discussions fostered by the work of the Expert Group in those past meetings and underscores the importance of the following recommendations.

I. Legislation and Frameworks

Recommendations:

- 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.

- 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.

- Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by capacity-building measures and technical assistance programs. 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.

- 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.

- 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.

II. Criminalization

Recommendations:

- 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.

- 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.

- 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.

- 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.

III. Law Enforcement and Investigations

Recommendations:

- 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.

- 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.

- 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, 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;

- 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.

- 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.

- 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.

IV. Electronic Evidence and Criminal Justice

Recommendations:

- 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 or multilateral treaty or in cooperation with the country that has jurisdiction.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 and prosecutors;
  (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;
  (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;
  (xiii) Strengthening of the technical and legal capacities of law enforcement agencies, judges and prosecutors through capacity-building and skill development programs;
  (xv) Holding of workshops and seminars to raise awareness of best practices in addressing cybercrime.

- In legal systems that use the inquisitorial model, where judicial officers are also investigators, the judiciary should receive specialized training on cybercrime.

- 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.

V. International Cooperation

Recommendations:

- Effective international cooperation requires national laws that create procedures that enable international cooperation. Thus, national laws must permit international cooperation among law enforcement agencies.

- 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.

- 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 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 international cooperation for many. Thus, countries should ensure that any new instrument on cybercrime avoids conflict with existing treaties.

VI. Prevention

Recommendations:

- 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.

- Public-private partnerships, including cooperation with cybersecurity stakeholders and technology companies on information-sharing, are needed to prevent and combat cybercrime.

- "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.

- Member States should avail themselves of capacity-building assistance from the UNODC Global Program on Cybercrime and other initiatives, including the Council of Europe Global Action on Cybercrime Extended programs.

- Efforts in the development of strategies for cybercrime prevention should also take into account the protection of human rights.

United Kingdom

Comments on Preliminary Conclusions and Recommendations of the Intergovernmental Expert Group (IEG) on Cybercrime

The Permanent Mission of the United Kingdom has the honour to respond to Note Verbale CU 2021/108(A)/DTA/OCB/CSS regarding the compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study on Cybercrime, held in 2018, 2019 and 2020.

The United Kingdom warmly welcomes the work of the IEG to date and wishes to provide the following comments on the conclusions and recommendations as well as the future work of the Expert Group for submission to the Commission on Crime Prevention and Criminal Justice (CCPCJ). The United Kingdom reaffirms its commitment to uphold international law, which applies in cyberspace as it applies to activities in any other domain.

Noting UN Member States collective commitment to tackling criminality, maintaining international peace and security, and to promoting and respecting human rights and fundamental freedoms for all, the United Kingdom has grave concerns about IEG recommendations moving beyond its mandate to discuss cybercrime and the criminal misuse of ICTs thereby cutting across the work addressed by other UN bodies and fora.

Issues related to ICTs in the context of international peace and security, including State behaviours, any discussion and clarification of how international law applies to the use of ICTs by States, the voluntary and non-binding norms, the protection of critical infrastructure from malicious cyber activity, and malicious cyber activity conducted by States or their proxies and possible responses are the subject of discussion among all UN Member States in the UN First Committee Open Ended Working Group, which concluded its report on 12 March; the new 5-year Open Ended Working Group, which is due to begin its work in June, as well as the UN Groups of Governmental Experts on advancing responsible state behavior in cyberspace in the context of international security.

The United Kingdom therefore objects to the inclusion of the following recommendations on the basis that they relate to matters of international peace and stability and fall outside the mandate of the IEG and the Third Committee in paragraphs 8 (f), (h), (m), (ee), and (iii) under International Cooperation and 9 (g), (u), (kk), (ll), (nn), and (pp) under Prevention.

Furthermore, in light of the serious and growing threat posed by cybercrime, the United Kingdom strongly believes there is a continued need for a format where experts can come together to analyse the problem in depth, through the exchange of information and operational experience, and seek to develop practical solutions in an environment free from political debate. The CCPCJ should consider extending the work plan of the IEG beyond 2021 as a forum for practitioners to exchange information on cybercrime and how best to tackle the problem together.

Additionally, the UK wishes to reiterate its support for existing international agreements to tackle cybercrime, including the Budapest Convention, which is a global treaty and open to all Member States. We also encourage all Member States to take full advantage of the UN Convention against Transnational Organised Crime.

The UK particularly welcomes the following recommendations

Legislation and Frameworks

1. 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.

2. 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.

3. 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.

4. 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.

5. 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;

Criminalization

1. Member States should take into account that many substantive criminal law provisions designed for "offline" crime may also be applicable to crimes committed online.

2. 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.

3. 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.

4. 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.

Law enforcement and investigations

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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;

Electronic evidence and criminal justice

1. 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.

2. 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.

3. 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.
4. 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.

5. 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;

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

International cooperation

1. 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

2. 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

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. Effective international cooperation requires national laws that create procedures that enable international cooperation. Thus, national laws must permit international cooperation among law enforcement agencies.

10. 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.

11. 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;

Prevention

1. Public-private partnerships, including cooperation with cybersecurity stakeholders and technology companies on information-sharing, are needed to prevent and combat cybercrime.

2. UNODC was strongly encouraged to continue providing technical assistance, upon request, to prevent and counter cybercrime.

3. Countries should collect a broad range of data to help understand trends to inform and shape cybercrime policies and operational responses to combat cybercrime.

4. "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.

5. 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.

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