United Nations E/CN.15/2018/6

Economic and Social Council

Distr.: General
22 February 2018

Original: English

Commission on Crime Prevention and Criminal Justice
Twenty-seventh session
Vienna, 14–18 May 2018
Item 5 of the provisional agenda*
Thematic discussion on criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels

Guide for the thematic discussion on criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels

Note by the Secretariat

Summary

The present guide for the thematic discussion on criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels, to be held by the Commission on Crime Prevention and Criminal Justice at its twenty-seventh session, has been prepared by the Secretariat pursuant to Commission decision 18/1. In its decision 2016/241, the Economic and Social Council decided that the prominent theme for the twenty-seventh session of the Commission would be entitled "Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels". In the present note, a series of questions on the relevant thematic areas are proposed for the thematic discussion, certain issues are outlined for shaping that discussion and background information is provided.

* E/CN.15/2018/1.

V.18-00973 (E) 060318 070318

I. Introduction

1. In its decision 2016/241, the Economic and Social Council decided that the prominent theme for the twenty-seventh session of the Commission on Crime Prevention and Criminal Justice would be entitled “Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels”.

2. At its reconvened twenty-sixth session, held on 7 and 8 December 2017, the Commission endorsed the proposal of the Chair regarding the approach to the organization of the thematic discussion at its twenty-seventh session as follows: the thematic debate would take place during a morning and an afternoon meeting. The morning’s debate would be devoted to the sub-theme “Current challenges”, and the afternoon’s debate to the sub-theme “Possible responses to them”.

3. The Secretariat has prepared the present note in accordance with Commission decision 18/1, entitled “Guidelines for the thematic discussions of the Commission on Crime Prevention and Criminal Justice”, in which the Commission decided that the discussion on the prominent theme would be based on a discussion guide including a list of questions to be addressed by participants.

II. Background information: setting the stage for the thematic discussion

4. While the rapid growth in Internet and computer technology has transformed societies around the world, they have also created new opportunities for crime. Computers, networks and data can be linked to various forms of crime in almost any conceivable way. They have become objects of crime and tools for crime at the same time and have given rise to new motives and opportunities for its expansion. They often tip the balance of risks and rewards for offenders in favour of the latter. Moreover, as a consequence of the underlying digital architecture of the Internet and the global availability of information and communications technology (ICT), cybercrime is linked to organized crime and is often transnational in nature.[1]

5. In its resolution 65/230, the General Assembly endorsed the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, as adopted by the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, and requested 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 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.

6. That mandate was renewed in the Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, adopted by the Thirteenth United

[1] *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (United Nations publication, Sales No. E.10.IV.6), p. 204; and *World Drug Report 2017: The Drug Problem and Organized Crime, Illicit Financial Flows, Corruption and Terrorism* (United Nations publication, Sales No. E.17.XI.11), p. 15.

Nations Congress on Crime Prevention and Criminal Justice and endorsed by the General Assembly in its resolution 70/174.

7. The Expert Group to Conduct a Comprehensive Study on Cybercrime has held a total of four meetings, in 2011, 2013, 2017 and 2018 respectively. In its resolution 22/7 of 26 April 2013, the Commission on Crime Prevention and Criminal Justice took note of the comprehensive study on cybercrime, prepared by the United Nations Office on Drugs and Crime (UNODC) under the auspices of the Expert Group and the discussion on its content at the second meeting of the Expert Group, held in Vienna from 25 to 28 February 2013 (see UNODC/CCPCJ/EG.4/2017/3) at which diverse views had been expressed regarding the content, findings and options presented in the study, and requested the Expert Group, with the assistance of the Secretariat, as appropriate, to continue its work towards fulfilling its mandate.

8. In its resolution 26/4, adopted at its twenty-sixth session, on 26 May 2017, the Commission on Crime Prevention and Criminal Justice requested the Expert Group to continue its work and, in so doing, to hold periodic meetings and function as the platform for further discussion on substantive issues concerning cybercrime, keeping pace with its evolving trends, and in line with the Salvador and Doha Declarations, and also requested the Expert Group to continue to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and propose new national and international legal or other responses to cybercrime. In the same resolution, the Commission decided that the Expert Group would dedicate its future meetings to examining, in a structured manner, each of the main issues dealt with in the study, without prejudice to other issues included in the mandate of the Expert Group, taking into account, as appropriate, contributions received pursuant to Commission resolution 22/7 and the deliberations of the previous meetings of the Expert Group.

9. In a wider context, there is an increasing recognition, as reflected in the 2030 Agenda for Sustainable Development adopted by the General Assembly in its resolution 70/1, that reducing conflict, crime, violence and discrimination, and ensuring inclusion, good governance and the rule of law, are crucial to securing sustainable development. Goal 16 of the 2030 Agenda (“Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels”) is of particular relevance in that regard. Goal 16 is linked to the fight against cybercrime, which, together with other forms of crime, including organized crime, undercuts good governance and the rule of law, threatens security and development, and has a destabilizing effect on Member States (see E/CN.7/2016/CRP.1-E/CN.15/2016/CRP.1, para. 4).

10. At the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice, to be held in Japan in April 2020, cybercrime aspects are to be addressed, among other issues, in the context of the fourth workshop of the Congress, on the topic “Current crime trends, recent developments, and emerging solutions, in particular new technologies as means for and tools against crime.”

11. Against that background, the thematic discussion on cybercrime to be held at the twenty-seventh session of the Commission is intended to take stock of recent developments. The thematic discussion is to serve as a platform for further discussion and an exchange of views and experiences among Member States. To facilitate the thematic discussion, eight thematic areas relevant to cybercrime have been identified, including areas that are explicitly included in the prominent theme. Each of those eight thematic areas is discussed separately in section III below, with separate subheadings for current challenges and possible responses (as agreed upon at the reconvened twenty-sixth session of the Commission, see para. 2 above) and an indicative list of questions or points for further discussion.

III. Thematic areas: issues for discussion

A. Types of cybercrime and related threats

Current challenges

12. “Cybercrime” is not a legal or forensic term, nor does it define or describe a clear category of criminal offences. There is general agreement on a core list of types of abuse and offences specifically related to computers, but beyond that there is still no global consensus on what the term means. This situation is the result of the ubiquitous nature of computers and their versatility, as well as of the dynamic evolution of ICT and the ways it has been used since the late 1950s.

13. Depending on the context, the term “cybercrime” can refer to crimes committed by means of ICT, crimes committed against ICT installations and their users as such, or criminal scenarios in which ICT plays an indirect or supporting role.[2] The term “cybercrime” has been used to describe a wide range of offences, including offences against computer data and systems (such as hacking), computer-related forgery and fraud (such as phishing), content offences (such as disseminating material relating to the sexual abuse of children)[3] and copyright offences (such as disseminating pirated content).

14. The increasing use of computer technology and the trend towards the digitalization of data have increased the relevance of computer data. As a consequence, computer data have become the target of frequent attacks that range from data interference to data espionage. There is now a sophisticated digital underground economy in which data are the commodity. Stolen personal and financial data — used, for example, to gain access to existing bank accounts and credit cards, or to fraudulently establish new lines of credit — have monetary value. This state of affairs drives a range of criminal activities, including phishing, pharming, malware distribution and the hacking of corporate databases, which are supported by a fully-fledged infrastructure of writers of malicious code, specialized web hosts and individuals able to lease networks of compromised computers to carry out automated attacks.

15. The development and distribution of malware, in particular, continues to be the cornerstone for the majority of cybercrime cases. Since late 2013, cryptoware (ransomware using encryption) has become the leading malware in terms of threat and impact. Following the trend of information stealers, cryptoware campaigns are increasingly targeting public and private sector entities.[4]

16. Criminals continuously seek methods and technologies to make their business models more effective and increase their profit margins. The anonymous nature of online transactions and the use of cryptocurrencies reduce the risk of detection by law enforcement authorities. The increased use of virtual private networks, onion routers and carrier-grade network address translation (where Internet protocol addresses are shared by several customers) limits the ability of investigators to attribute evidence.

17. Cybercrime rates continue to increase in line with the expansion of the Internet, thereby raising the vulnerability of Internet users to new levels. Furthermore, the threat posed by cybercrime in its different forms is multidimensional, targeting not only citizens, but also businesses and Governments at a rapidly growing rate.

---

[2] Christopher Ram, “Cybercrime” in *Routledge Handbook of Transnational Criminal Law*, Neil Boister and Robert J. Currie, eds. (New York, Routledge, 2015), p. 379.

[3] See United Nations Office on Drugs and Crime, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, (Vienna, 2015).

[4] European Police Office, *European Union Serious and Organised Crime Threat Assessment: Crime in the Age of Technology* (The Hague, 2017), p. 30.

Cybercrime tools pose a direct security threat and play an increasingly important role in facilitating most forms of organized crime and terrorism.

Possible responses

18. The unprecedented scale of the problem, coupled with the multiple types of conduct described as cybercrime, threaten the ability of authorities to respond effectively and efficiently. At the same time, cyberspace may also offer opportunities and tools for detecting cybercrime. The use of ICT by offenders can generate a number of investigative and evidential leads for the criminal justice system. Authorities have more data on criminal activity at their disposal than ever before, and now have an opportunity to harness that information in ways that make gathering intelligence and investigation cost-effective. An interesting example is that of the criminal exploitation of cryptocurrencies. Cryptocurrencies are made possible by blockchain technology. In spite of the currently existing technical and legal loopholes, several aspects of blockchain technology could make it a useful law enforcement tool to look for suspicious transaction patterns and track evidence (see E/CN.15/2018/CRP.1, para. 164).

19. Skilled digital investigators trained through enhanced capacity-building efforts are able to acquire electronic evidence of cybercrime, even when perpetrators carefully avoid leaving digital traces or erase them. Depending on data retention times, Internet protocol connection logs may be consulted to establish times, sources and destinations of Internet connections.

20. Moreover, the increasing dependence of society on the Internet and computer-assisted communication has led law enforcement to develop tools to investigate offences online or to use, for example, software to reveal criminal patterns. Law enforcement agencies also use social media tools to improve their relationships with local communities and to ask the public for its cooperation in criminal investigations.

21. It is therefore essential for States to consider developing multidisciplinary strategies to address the challenges and upgrade their capacity for successful and effective investigation and prosecution in cases involving cybercrime. Multidisciplinary strategies can range from regulatory measures and policymaking initiatives to cybercrime prevention and the training of competent authorities, as discussed below.

Points for discussion

22. The Commission may wish to consider the following points for further discussion:

(a) What are the lessons learned from the analysis of evolving patterns in cybercrime?

(b) What is the best way to use those lessons for shaping effective regulatory responses to and policymaking strategies against cybercrime at the national level?

(c) What is the impact of various types of cybercrime on the capacity of Member States to keep systematic records of related offences and to exchange information for law enforcement purposes at the regional and international levels, including information about the involvement of organized criminal groups, the modi operandi of such groups and the techniques utilized in the identification of forms of cybercrime?

(d) To what extent can the definitions given in the United Nations Convention against Transnational Organized Crime of the terms “organized criminal group” and “structured group” be applied to cyberspace, including in cases where offenders, often protected by anonymity, interact without knowing who the other is?

B. Legal measures against cybercrime: criminalization aspects

Current challenges

23. When evaluating the current challenges in developing legal responses to cybercrime, it is useful to bear in mind how these challenges emerged and escalated throughout the years. Historically, computer-related services and Internet-related technologies gave rise to new forms of crime soon after they were introduced. One example is the development of computer networks in the 1970s and the first unauthorized access to computer networks, which occurred shortly afterwards. Similarly, the first software offences appeared soon after the introduction of personal computers in the 1980s, when personal computers were used to copy software products. By the late 1990s, networks had become a critical part of ICT infrastructure, which led to increasing concerns about certain forms of cybercrime threatening them. This, in turn, led to the use of cybersecurity and a trend to specifically criminalize, or provide for aggravated penalties for, certain types of attacks against critical infrastructure.[5]

24. Apart from the emergence of new definitions and concepts based on rapidly evolving technologies, there has been the persistent question of whether to treat cybercrime as a new phenomenon and create entirely new offences relating to it, or to attempt to apply existing definitions of offences and, if necessary, expand or adjust them. Some countries have enacted new legislation treating computer fraud as a specific offence, while others have introduced the illicit copying or damaging of data, impeding access to data or the improper use of data as new offences because existing definitions related only to tangible property. Another example is the establishment of identity theft as a specific offence in some jurisdictions.

25. Where adjustments to pre-existing criminal legislation are preferred, legislatures often struggle with lengthy procedures to review and update the law. The main challenge, therefore, is the delay between the discovery of new forms of criminal abuse and the enactment of the legislative amendments needed to cope with them. This challenge remains as relevant and topical as ever as the innovation of ICT accelerates.

Possible responses

26. Appropriate criminal legislation is the foundation of the investigation and prosecution of cybercrime. Therefore, lawmakers should be able to respond to ICT developments and monitor the effectiveness of existing legal provisions continuously. A thorough analysis of current legislation is necessary to identify possible gaps and address resulting difficulties in meeting the double criminality requirement in the context of international cooperation. Legislators may also benefit from binding and non-binding multilateral instruments.

27. To have a lasting effect, new laws and amendments to existing laws may need to be drafted flexibly and be technologically neutral, taking into account the need for legal certainty and precision. Laws should also address the need for timely access to information across national boundaries. Finally, legislators may require sufficient training and guidance so that they formulate sound provisions and enact effective laws.

---

[5] See, inter alia, Aunshul Rege-Patwardhan, “Cybercrimes against critical infrastructures: a study of online criminal organization and techniques”, *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, vol. 22, No. 3 (2009), p. 261; Luca Montanari and Leonardo Querzoni, eds., *Critical Infrastructure Protection: Threats, Attacks and Countermeasures* (March 2014). See also Security Council resolution 2341 (2017) on the threats to international peace and security caused by terrorist acts.

Points for discussion

28. The Commission may wish to consider the following points for further discussion:

(a) What are the lessons learned from efforts at the national level to develop and enforce legislation against cybercrime and to integrate that legislation within the broader framework of a national cybercrime strategy?

(b) Do national laws provide a sufficient legal basis for the effective detection, investigation and prosecution of all offences related to cybercrime? What are the gaps that need to be addressed?

(c) What is the impact of existing multilateral instruments on the scope of national legal frameworks against cybercrime? Has convergence of national legal responses based on such instruments been achieved and, if so, to what extent?

(d) In view of the dual criminality requirement, does the diversity of national approaches to the criminalization of cybercrime offences have an impact on the scope of international cooperation?

C. Procedural powers and electronic evidence

Current challenges

29. National investigative powers play a key role in gathering electronic evidence. An examination of investigative powers at the national level reveals a considerable diversity in the approaches to using electronic evidence to investigate crime. Those relate to the extent to which pre-existing powers can be interpreted to apply to data as non-tangible evidence and the legal authority that exists for particularly intrusive measures, such as remote forensic investigations. While legal powers vary, a corpus of specific investigative measures should be available for gathering electronic evidence. Such measures may include the expedited preservation of computer data; orders for access to stored content data; orders for access to stored traffic data; orders for access to subscriber information; real-time collection of content data; real-time collection of traffic data; search for computer hardware or data; seizure of computer hardware or data; trans-border access to a computer system or data; and use of remote forensic tools. Examples of national laws on investigative measures can be found in the UNODC Cybercrime Repository and the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal. Investigative powers need to keep pace with modern technologies. They should be supported by legal and institutional frameworks that facilitate timely and effective coordination and cooperation between the private sector and relevant government agencies at the national, regional and international levels while observing human rights. It is vital that those frameworks have a strong human rights component, as ICT affects areas such as privacy and freedom of expression.

30. Ideally, electronic evidence is admissible in court. However, the increasing relevance of electronic evidence in criminal proceedings presents challenges that were previously unknown. For instance, electronic evidence is highly fragile and can easily be modified or deleted. As a consequence, one of the key steps in computer forensics is to safeguard the integrity of electronic evidence. Protecting data integrity is also necessary to ensure the reliability and accuracy of the evidence. In addition, in order to be admissible, electronic evidence should be gathered through established procedures that safeguard human rights.

31. Moreover, for law enforcement authorities to effectively investigate and gather electronic evidence related to cybercrime, cooperation with other relevant actors, including from the private sector, has gained particular importance over the last years.

Overall, communication service providers play an important role in the accessibility of electronic evidence. National privacy laws can affect the ability of providers to share information with the authorities as part of an investigation.

Possible responses

32. Because electronic evidence is volatile, certain standards and requirements are needed for handling it and for ensuring its authenticity and integrity. Those standards and requirements include general rules and procedures, such as the keeping of case records, the use of widely accepted technology and the involvement of qualified experts in investigations.

33. An increasing number of cybercrime investigations, including into cases involving child abuse and exploitation, require electronic evidence held by third parties. It is therefore critical that industry and Governments work together to develop mechanisms giving law enforcement timely access to data in emergency situations. Such mechanisms ought to be combined with fair and transparent legal processes for routine investigations.

34. An expert group meeting on lawful access to digital data across borders, jointly organized by UNODC and the Counter-Terrorism Committee Executive Directorate in cooperation with the International Association of Prosecutors, was held in Vienna on 12 and 13 February 2018. The aim of the meeting was to set the basis for the development of a practical guide for central authorities, prosecutors and investigators for obtaining electronic evidence from foreign jurisdictions in cross-border counter-terrorism and related organized crime investigations. The meeting offered an opportunity to share national laws and guides, and examples of real-life cases that demonstrated good practices in and lessons learned from obtaining electronic evidence from communication service providers located in foreign jurisdictions.

Points for discussion

35. The Commission may wish to consider the following points for further discussion:

(a) What challenges do investigating authorities encounter when trying to meet the requirements for using special investigative techniques and for gathering and sharing electronic evidence to detect, investigate and prosecute cybercrime, and what are good practices in responding to those challenges?

(b) What experience has been accumulated in Member States with the admissibility of such evidence in court?

(c) What is the impact of collaboration with the financial sector in collecting electronic evidence relating to the proceeds of cybercrime (e.g. money mules)?

(d) What are the main challenges, from the perspective of the rule of law and human rights, in the effective use and implementation of techniques related to the investigation and prosecution of cybercrime?

(e) What are the lessons learned from efforts to foster cooperation between law enforcement authorities and communication service providers to secure electronic evidence for the detection, investigation and prosecution of cybercrime?

D. Jurisdictional issues

Current challenges

36. International law provides for a number of bases of jurisdiction over acts of cybercrime, primarily forms of territory- and nationality-based jurisdiction. Some of those bases can be found in multilateral cybercrime instruments. Extended or

objective territorial jurisdiction is now often based on the occurrence of an element of an offence, its effects or some other significant link to a State's territory. States must also determine which country is in the best position to prosecute alleged offenders based on factors such as the location of the evidence or the offenders.

37. The application of a range of jurisdictional bases by different countries can lead to more than one country asserting jurisdiction over the same act of cybercrime. The risk of jurisdictional conflicts increases even further if the principle of territoriality is applied to cases where only the infrastructure used for the commission of a crime is located in the relevant country, not the offender or the victim.

38. Cloud computing raises a number of challenges for criminal justice, in particular with regard to the applicable law and the criminal jurisdiction to enforce. It is often unclear to criminal justice authorities in which jurisdiction the data are stored and what legal regime applies to them. A service provider may have its headquarters in one jurisdiction but be subject to the legal regime of a second jurisdiction while the data are stored in a third jurisdiction. The same data may be kept in several jurisdictions using a technique known as mirroring, or they may move between jurisdictions, thereby further complicating these issues.

39. Moreover, it is often not clear whether a provider of cloud computing services is the controller or the processor of data that belong to a user and, thus, it is not clear which rules apply. Another factor of uncertainty is whether data are stored or are in transit and, thus, whether and on what jurisdictional basis production orders, search and seizure orders, interception orders or real-time collection orders are to be served. Furthermore, the non-localized nature of cloud computing causes problems for online forensics and searches because of the architecture of the cloud (multitenancy, distribution and segregation of data), and because of legal challenges related to the integrity and validity of the data collection, evidence control, ownership of the data or jurisdiction.[6]

Possible responses

40. In many cases, several States can claim jurisdiction over cybercrime offences and it is important to hold consultations to decide which State should prosecute. That decision may involve legal, diplomatic and practical issues, such as the jurisdictional and other legal claims made by each State, the question whether offenders can be extradited to the State that wishes to conduct the prosecution, and pragmatic considerations such as cost and other obstacles standing in the way of transferring evidence from one State to another, ensuring that the evidence is admitted in court and effectively presenting the evidence before the court. Where they arise, jurisdictional conflicts are typically resolved through formal and informal consultations between countries. Where it is decided that one of several possible States should prosecute, the jurisdiction of other States can effectively be transferred. The transfer of criminal proceedings, as a distinct form of international cooperation, provides the context and the framework to do so.[7]

41. Work to strengthen international and regional cooperation to secure electronic evidence has also been done at the multilateral level. In June 2017, the Cybercrime Convention Committee of the Council of Europe approved the preparation of a second protocol to the Convention on Cybercrime aimed at providing clear rules and more effective procedures to secure electronic evidence "in the cloud" in specific criminal

[6] Council of Europe, Cybercrime Convention Committee (T-CY), "Criminal justice access to data in the cloud: challenges", discussion paper prepared by the T-CY Cloud Evidence Group, 26 May 2015, document T-CY (2015)10, pp. 10–14.

[7] See background paper prepared by the Secretariat on practical considerations, good practices and challenges encountered in the area of transfer of criminal proceedings as a separate form of international cooperation in criminal matters (CTOC/COP/WG.3/2017/2).

investigations. The terms of reference were approved on 8 June 2017 and negotiations are scheduled to take place from September 2017 to December 2019.

Points for discussion

42. The Commission may wish to consider the following points for further discussion:

(a) What are the criteria that govern jurisdiction for purposes of enforcing criminal justice responses in cybercrime cases? How are those criteria applied to cloud computing scenarios where the data are often not “at rest”?

(b) What experience has been accumulated in conducting consultations to resolve jurisdictional conflicts over cybercrime offences? What are the challenges, what are good practices and what lessons have been learned?

E. Inter-agency coordination and cooperation at the national level

Current challenges

43. Multi-stakeholder cybercrime strategies are a vital element in the fight against cybercrime. The legal, technical and institutional challenges posed by cybercrime are far-reaching and can only be addressed by following a coherent strategy rooted in existing initiatives and the role of different stakeholders. To be effective, the fight against cybercrime requires highly developed organizational structures that avoid overlap and have clearly defined competences, that can coordinate all parties involved so that they can take concerted action. Without the right structures, it will be exceptionally difficult to implement robust policies and programme initiatives.

44. Deterring cybercrime is also an integral component of national strategies to ensure cybersecurity and protect critical information infrastructure. That includes, in particular, the adoption of legislation to combat the misuse of ICT for criminal and other purposes and to counter activities intended to compromise the integrity of critical national infrastructure. Deterring cybercrime is a shared responsibility of government authorities, the private sector and citizens requiring their coordinated action to prevent, prepare for, respond to and recover from cybersecurity incidents. The formulation and implementation of a national strategy against cybercrime requires a comprehensive approach, one that involves collaboration and coordination among relevant stakeholders at the institutional level.

45. Nevertheless, institutional coordination poses a number of difficulties, most of which are related to the resources and capabilities each country has at its disposal. Several other factors need to be taken into account, including the extent of private sector support, for example through public-private partnerships, or the self-regulation and self-protection measures the private sector has in place.

Possible responses

46. The establishment of multi-agency partnerships has emerged as a common practice for combating cybercrime, including technology-facilitated crimes against children, at the strategic level. In response to the multifaceted challenges encountered in the fight against cybercrime, communication service providers and public institutions such as law enforcement and criminal justice authorities need to create public-private partnerships in which they can build trust and two-way dialogues. More broadly, States need to mount regulatory responses that go beyond criminal law and provide incentives for the private sector to get actively involved in crime prevention. Such an approach may be useful in creating an environment that is sensitive to emerging threats and conducive to countering them.

47. Task forces that target Internet-facilitated organized crime could be a useful tool for taking concerted action against cybercrime. Such task forces should be responsive to the evolving criminal environment and could lead to the creation of, for example, more permanent groups for sharing information and more ad hoc arrangements for specific operations such as dismantling botnets. In all cases, authorities need to have the flexibility to involve a variety of stakeholders, such as law enforcement, the private sector, academia and user groups, and to coordinate efficiently with them to achieve the desired outcome.

48. The Internet has further changed the focus of government ICT regulation within Governments. Authorities regulating the ICT sector already find themselves involved in a range of activities to address cybercrime. This is the case, in particular, in areas such as content regulation, network safety and consumer protection, as users have become vulnerable. The involvement of regulators is therefore the result of the fact that cybercrime undermines the development of the ICT industry and of parties offering related products and services. The new duties and responsibilities of ICT regulators in combating cybercrime can be seen as part of the wider trend towards the conversion of centralized models of cybercrime regulation into flexible structures.[8]

Points for discussion

49. The Commission may wish to consider the following points for further discussion:

(a) What challenges are encountered at the national level in strengthening institutional capacities and inter-agency coordination to address cybercrime?

(b) Has any experience been accumulated in developing model frameworks or guidelines for cooperation among relevant stakeholders at the national level to prevent and combat cybercrime? If so, how did such model frameworks or guidelines foster actual collaboration?

F. International cooperation

Current challenges

50. In addition to criminalizing acts of cybercrime and granting related procedural powers, existing instruments set out mechanisms for international cooperation in the cross-border investigation and prosecution of cybercrime. International cooperation to combat cybercrime represents an increasing challenge for criminal justice and law enforcement authorities. While, theoretically, the location of specific computer data may be identifiable at a particular point in time, the advent of cloud computing, encryption and peer-to-peer data-sharing and storage has meant that the data may now exist in the form of multiple copies distributed across multiple devices and locations, and that they may be moved to another geographical location in a matter of seconds.[9]

51. Owing to the volatile nature of electronic evidence, international cooperation in cybercrime matters requires a timely response, including the preservation and production of data by service providers, and the ability to request specialized investigative action. One challenge commonly encountered when requesting such data from another jurisdiction are delays in the response that often exceed the data retention period and may enable perpetrators to permanently destroy key electronic evidence. Other common challenges include a lack of commitment and flexibility on

[8] International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (Geneva, 2012), p. 101.

[9] Background paper on workshop 3 on strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation (A/CONF.222/12), para. 32.

the part of the requested authority, whether that authority provides the evidence in a form that can be used in criminal proceedings, and differences in the definitions of criminal offences in cooperating States.[10]

52. At the second meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in 2013, most experts agreed that increased and faster international cooperation would be needed to address the problem of cybercrime, especially as that problem continued to expand and reliance on technologies for legitimate purposes made the potential threat of cybercrime more serious. Beyond that, different views were expressed regarding the best strategic approach and priorities for addressing the problems related to cybercrime.[11] In that context, there has been a controversy over whether a new universal legal instrument against cybercrime should be created to address, among other things, international cooperation aspects at a global level, or, instead, the international community should continue to rely on existing multilateral instruments, including the Council of Europe Convention on Cybercrime. The matter continues to be debated without a consensus having been reached to date.

Possible responses

53. International cooperation mechanisms could be improved further by examining how mutual legal assistance processes may be expedited. Other solutions may lie in strengthening law enforcement cooperation and continuing the multilateral dialogue on transnational access to computer data. For example, establishing a separate regime for access to subscriber information as defined in article 18, paragraph 3 of the Council of Europe Convention on Cybercrime, differentiating between the types of data sought, could greatly contribute to making mutual legal assistance in matters of cybercrime and electronic evidence more efficient.[12]

54. Innovations such as the inclusion of an electronic evidence module in the redeveloped UNODC Mutual Legal Assistance Request Writer Tool may assist in streamlining mutual legal assistance processes involving electronic evidence. In parallel, however, law enforcement may increasingly need to find pioneering ways of collaborating in transnational cybercrime investigations. The involvement of entities such as the Global Complex for Innovation of the International Criminal Police Organization (INTERPOL) and the European Cybercrime Centre of the European Police Office (Europol) in coordinating and supporting transnational investigations, including by facilitating information-sharing between national law enforcement authorities, may prove especially important in that regard.

55. Other solutions may include the following: establishing separate cybercrime units within central authorities; monitoring and reviewing casework practices in matters of mutual legal assistance for responsiveness and efficiency, including through keeping statistics of requests for mutual legal assistance involving electronic evidence; more frequent use of police-to-police cooperation as a useful supplement to mutual legal assistance modalities to ensure timely responses to urgent requests for assistance; focused and more intensive training to enhance mutual legal assistance, police-to-police and other forms of international cooperation on cybercrime and electronic evidence; enhanced sharing of information and experience among 24/7 networks of contact points; and allocating resources at the level of national

[10] See background paper prepared by the Secretariat on gathering and sharing electronic evidence (CTOC/COP/WG.3/2015/2), para. 19.

[11] Deliberations at the second meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 25 to 28 February 2013, Summary by the Rapporteur, UNODC/CCPCJ/EG.4/2017/3, para. 25.

[12] See Council of Europe, Cybercrime Convention Committee, Cloud Evidence Group, “Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY”, document T-CY (2016)5, p. 13.

authorities entrusted with the task of executing requests for mutual legal assistance, and enhancing their coordination with the central authorities for timely responses.

Points for discussion

56. The Commission may wish to consider the following points for further discussion:

(a) How can the timeliness of mutual legal assistance procedures be improved in cases involving cybercrime and electronic evidence? What are the best practices and where lie the challenges in police-to-police cooperation when taking electronic evidence abroad?

(b) What examples can States provide of how intensifying information-sharing at the regional and international levels has increased the capacity to detect and assess risks and respond to requests effectively and in a timely manner?

(c) How should international requests for preservation of electronic evidence be prepared, transmitted and processed? What experience has been accumulated with public-private sector cooperation in that regard?

G. Prevention of cybercrime

Current challenges

57. The costs and complexity of investigating and prosecuting cybercrime cases suggests that the benefits of cooperative prevention efforts may be substantial. Public-private partnerships, in particular, are central to cybercrime prevention. Service providers can play a role in cybercrime prevention by: (a) storing user data that law enforcement officials in possession of a warrant can access for use in cybercrime investigations; and (b) actively filtering Internet communications and content with a view to preventing cybercrime acts before they are committed. When analysed within the context of freedom of speech, however, those two measures raise numerous challenges.

58. When discussing the role of service providers in preventing cybercrime, consideration may need to be given to their limitations as private sector entities. Firstly, provider policies are often volatile and lack foreseeability for law enforcement as well as customers. Service providers may change their policies unilaterally at any time and without prior notice to law enforcement. Adding to this, policies and practices not only differ widely between providers, but also with respect to different Member States. One provider may respond to many requests from one country but to none or a few from another, while the practices of another provider may be exactly the opposite.[13]

59. Secondly, police cybercrime investigations may be affected by data protection safeguards that require personal data to be deleted when no longer required for the purposes for which they were collected. Thus, while data retention laws may represent a pragmatic approach to ensuring that communication service providers are able to play a greater role in cybercrime prevention through enhanced cooperation with law enforcement, it is important that such laws are implemented with due procedural safeguards and privacy protections. Standards and regulations on data protection need to be taken into account, including the general data protection regulation of the European Union.[14]

---

[13] Ibid., “Criminal justice access to data in the cloud: Cooperation with ‘foreign’ service providers”, (T-CY (2016)2), p. 22.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*Official Journal of the European Union*, L 119, 4 May 2016, pp. 1–88).

60. Academia faces the considerable challenge of filling in the many gaps that exist and continue to emerge in the knowledge on cybercrime, in particular ICT-related sexual abuse and exploitation of children. Subject to sustainable funding, which in many jurisdictions represents a significant challenge, academic institutions can play a variety of roles in preventing cybercrime, including through the delivery of education and training to professionals, law and policy development, work on technical standards and solution development.

Possible responses

61. Good practices in cybercrime prevention include the promulgation of legislation, effective leadership, the development of criminal justice and law enforcement capacity, the development of a strong knowledge base, and cooperation between government, communities, the private sector and States. It is of utmost importance to provide assistance in developing and refining preventive techniques, share lessons learned and best practices, and share the information needed to develop preventive techniques and make them effective.

62. Awareness-raising and educational campaigns and initiatives, including those covering emerging threats and those targeted at specific audiences such as children, has been highlighted as an important component of policies to prevent cybercrime.[15] The Education for Justice initiative, a key component of the UNODC Global Programme for the Implementation of the Doha Declaration includes the development and dissemination of counter-cybercrime materials for children and young people in the primary, secondary and tertiary levels of education.

63. Civil society can play a vital role in helping children to understand and handle online risks, which is of particular importance in efforts to prevent ICT-facilitated child abuse and exploitation. Education and psychosocial prevention methods are acknowledged as essential in protecting children from ICT-facilitated abuse and exploitation. Education initiatives enable children, their families and other caregivers to understand and correctly assess the risks associated with ICT.[16]

64. A number of models exist for public-private partnerships that foster the prevention of cybercrime, such as those between law enforcement authorities and communication service providers. Many rely on information-sharing on the basis of clear rules, trust, restricted membership, the encouragement of mutual benefits, and responsiveness. Furthermore, the role of the private sector in identifying and blocking, inter alia, online material relating to the sexual abuse of children before customers can access it, will continue to grow.[17]

65. A clear, forward-looking approach for Governments is to work in partnership with those who will influence the future business and operating environment, so that all concerned can better anticipate changes in criminal behaviours and technological misuse. In that context, it will be important to continue to develop insights into the behaviour of the contemporary cybercriminal by means of intelligence analysis, criminological research and profiling techniques in order to deploy existing resources more effectively and proactively identify features of future communications technologies vulnerable to criminal exploitation.

[15] See *Study on the Effects of New Information Technologies*, p. 54.
[16] Ibid., p. 54.
[17] See, for example, *The Netclean Report 2017*, available at https://www.netclean.com/netclean-report-2017.

Points for discussion

66. The Commission may wish to consider the following points for further discussion:

(a) What examples can States provide of effective prevention strategies among relevant stakeholders against cybercrime? How is success defined and measured?

(b) How can academic institutions, the private sector and non-governmental organizations best contribute to the development and sharing of knowledge, legislation and policy in the area of cybercrime?

(c) What is the accumulated experience of Member States with regard to balancing data protection and the effectiveness of investigations into cybercrime?

H. Capacity-building and technical assistance

Current challenges

67. Capacity-building at the level of national law enforcement and criminal justice systems is critical. While the majority of countries have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence, in many countries those structures are underfunded and suffer from a lack of capacity. As electronic evidence is essential in the investigation of cybercrime, law enforcement authorities may need to make clear distinctions between, and establish clear workflows for, cybercrime investigators and digital forensic laboratory capacity. Front-line law enforcement officers may increasingly need to acquire and deploy basic skills, such as those used to produce a forensically sound image of an electronic storage device.

68. Overall, it is clear that building the capacity of law enforcement and criminal justice actors to combat cybercrime will be an ongoing and continuous process, as technology and criminal innovations continue at a rapid pace.

Possible responses

69. Technical assistance and cooperation are important to enable the sharing of good investigative practices, experience and the dissemination of new techniques. Member States may wish to enhance the sharing of new approaches to the investigation of complex, Internet-based financial fraud, online drug trafficking or the use of virtual currencies for money-laundering, thereby enabling law enforcement authorities in various countries to rapidly acquire the necessary skills to counter emerging cybercrime threats.

70. Specialized cybercrime structures or units within law enforcement agencies can make it easier for States to concentrate limited resources in a single place in order to build specialized investigative techniques and to gather and analyse suitable electronic evidence, including by conducting digital forensic examinations. At the same time, such structures or units may provide training for local law enforcement agencies, coordinate national responses to cybercrime, facilitate cooperation among partners involved in the investigations, and target forms of cybercrime that may be of particular concern to a State.

71. In line with General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8, UNODC, through its Global Programme on Cybercrime, is mandated to assist Member States in their struggle against cybercrime through capacity-building and technical assistance. Under the Programme, UNODC provides focused technical assistance for capacity-building, prevention and awareness-raising, international cooperation and analysis in

relation to cybercrime, principally in developing countries. It also provides, upon request and within its mandate, legislative assistance to Member States in need.

72. As an example, UNODC has developed a train-the-trainers course on cryptocurrency investigation and has been delivering cryptocurrency investigation training in various regions. The aim of the training is to upgrade the capacity of law enforcement officers, analysts, prosecutors and judges in relation to cryptocurrencies, tracing bitcoins in a financial investigation, locating information resources and collaborating on international casework.

Points for discussion

73. The Commission may wish to consider the following points for further discussion:

(a) Which aspects of cybercrime-related measures and strategies have high priority for technical assistance and capacity-building, in particular in view of the evolving nature of cybercrime and the new and emerging threats associated with it?

(b) What lessons have been learned from the sharing of good investigative practices, from experience and from the dissemination of new techniques as an example of technical assistance cooperation?

(c) How can synergies and alliances be best pursued and promoted between international organizations delivering technical assistance in matters of cybercrime for the delivery of tangible and sustainable capacity-building services to Member States in need of assistance?

IV. Addressing current gaps and the way forward

74. Efforts made by the international community to better understand and respond to cybercrime threats continue to increase. Nonetheless, more work is urgently needed as significant challenges remain in the development and implementation of comprehensive, coordinated, sustainable and effective responses to cybercrime.

75. By facilitating the thematic discussion at its twenty-seventh session, the Commission, during its deliberations on the relevant agenda item, will serve as a platform for the exchange of information, best practices and lessons learned, developing effective responses and promoting relevant international instruments or standards in countering cybercrime.

76. In considering further action to address the challenges posed by cybercrime and the way forward to developing appropriate responses, the Commission may wish to focus the discussion on areas in current national legal and institutional frameworks that are perceived to present the greatest risk, and on priority areas where Member States face the greatest challenges.

77. The Commission may consider recommending that Member States further strengthen their capacity-building efforts and legal frameworks, in particular when reviewing existing national policies, laws and institutional frameworks with the objective of identifying new or amended legislation, institutional frameworks and practices that might strengthen their capacity to address existing and emerging cybercrime threats.

78. The Commission may identify and prioritize areas of technical assistance that UNODC might undertake in close collaboration and coordination with other relevant actors, on the basis of relevant mandates, to better support Member States in the implementation of national policies, laws and institutional capacities to address current and emerging challenges relating to cybercrime.

79. The Commission may further wish to invite UNODC to assist it in maintaining communication with other intergovernmental bodies dealing with cybercrime and criminal justice responses to prevent and counter it, including the Conference of the Parties to the Organized Crime Convention and its Working Group on International Cooperation, within their respective mandates and as appropriate.