United Nations E/CN.15/2020/12

Economic and Social Council

Distr.: General
17 March 2020

Original: English

**Commission on Crime Prevention and Criminal Justice**
**Twenty-ninth session**
Vienna, 18–22 May 2020
Item 6 (d) of the provisional agenda*
**Integration and coordination of efforts by the United Nations Office on Drugs and Crime and by Member States in the field of crime prevention and criminal justice: other crime prevention and criminal justice matters**

# Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing

## Report of the Secretary-General

*Summary*

The present report was prepared pursuant to General Assembly resolution 74/173, entitled "Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing", in which the General Assembly requested the Secretary-General to report to the Commission on Crime Prevention and Criminal Justice at its twenty-ninth session on the implementation of that resolution.

The report describes progress made in 2019 by the United Nations Office on Drugs and Crime in promoting and delivering technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing.

* E/CN.15/2020/1.

# I. Introduction

1. In its resolution 64/179, adopted in 2009, the General Assembly drew attention to cybercrime as an emerging policy issue, with particular reference to the technical cooperation activities of the United Nations Office on Drugs and Crime (UNODC), and invited the Office to explore, within its mandate, ways and means of addressing the issue.

2. In 2010, in its resolution 65/230, the General Assembly requested UNODC, in the development and implementation of its technical assistance programmes, to aim for sustainable and long-lasting results in the prevention, prosecution and punishment of crime, in particular by building, modernizing and strengthening criminal justice systems, as well as promoting the rule of law, and to design such programmes to achieve those aims for all components of the criminal justice system, in an integrated way and with a long-term perspective, increasing the capacity of requesting States to prevent and suppress the various types of crime affecting societies, including organized crime and cybercrime.

3. In 2011, in its resolution 20/7, the Commission on Crime Prevention and Criminal Justice requested UNODC, in cooperation with Member States, relevant international and regional organizations and, as appropriate, the private sector, to continue to provide, upon request, technical assistance and training to States, based on national needs, especially with regard to the prevention, detection, investigation and prosecution of cybercrime in all its forms.

4. Furthermore, in 2013, in its resolution 22/8, the Commission on Crime Prevention and Criminal Justice invited UNODC to advance the implementation of the Global Programme on Cybercrime and requested it to strengthen partnerships for technical assistance and capacity-building to counter cybercrime with Member States, relevant organizations, the private sector and civil society.

5. In 2019, in its resolution 74/173, the General Assembly requested UNODC to continue to provide, upon request and based on national needs, technical assistance and sustainable capacity-building to Member States to deal with cybercrime, through the Global Programme on Cybercrime and, inter alia, its regional offices, in relation to the prevention, detection, investigation and prosecution of cybercrime in all its forms, recognizing that cooperation with Member States, relevant international and regional organizations, the private sector, civil society and other relevant stakeholders can facilitate this activity.

6. In response, UNODC – primarily through its Global Programme on Cybercrime provides technical assistance and capacity-building on cybercrime to Member States at the national, regional and global levels. UNODC also functions as technical secretariat to the Expert Group to Conduct a Comprehensive Study on Cybercrime. Efforts to prevent cybercrime are also supported to a significant degree by the UNODC Global Programme for the Implementation of the Doha Declaration, through its Education for Justice initiative.

7. In planning and implementing its activities to counter cybercrime, UNODC closely cooperates with, guides and advises key cybercrime partners and forums such as the International Criminal Police Organization (INTERPOL), the International Telecommunication Union, the European Union Agency for Law Enforcement Cooperation, the European Cybercrime Training and Education Group, the World Bank, the United Nations Children's Fund (UNICEF), the Association of Southeast Asian Nations (ASEAN), the World Internet Conference, End Violence and the Global Forum on Cyber Expertise.

8. In 2019, UNODC continued to provide holistic support to Member States to prevent, detect, investigate and prosecute cybercrime in all its forms, with due regard for human rights and fundamental freedoms in the use of information and communications technologies. This includes, for example, the proportionate, legal, accountable and necessary acquisition and use of digital forensic evidence.

9. Throughout the reporting period, and in line with the priorities of the Secretary-General's strategy on new technologies, UNODC continued to support the work of the General Assembly, the UNICEF working group on cryptocurrency and the High-level Panel on Digital Cooperation. Furthermore, the Office routinely provided guidance and advice on the impact of cybercrime on cybersecurity and peace and security.

# II. New developments, progress made and best practices identified

10. In accordance with General Assembly resolution 73/187, on countering the use of information and communications technologies for criminal purposes, the Secretary-General submitted a report (A/74/130) setting out the views of Member States on the challenges that they faced in countering the use of information and communications technologies for criminal purposes. The report reflected the views of 61 reporting Member States, in the form of summaries prepared by the Secretariat. Submissions by Member States covered challenges at both the national and international levels, as well as actions taken to address those challenges. Member States also provided information on technical and technology-related challenges and shared their experiences in tackling them. The importance of international cooperation in countering the use of information and communications technologies for criminal purposes was also highlighted.

11. UNODC has been following the developments relating to the adoption of General Assembly resolution 74/247, on countering the use of information and communications technologies for criminal purposes, which includes a mandate for the establishment of an open-ended ad hoc intergovernmental committee of experts that represents all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. In that context, UNODC will provide substantive and administrative support to the organizational session of the committee, to be held in New York in August 2020.

# III. Normative and capacity-building support

12. Cybercrime mentors based in Austria, El Salvador, Guatemala, Kenya, Senegal and Thailand continued to support countries in countering cyber-dependent and cyber-enabled crimes and handle and exchange electronic evidence. Moreover, in 2019, UNODC capacity-building efforts continued to address the needs of developing countries, focusing on their self-identified vulnerabilities in order to provide tailor-made technical assistance and promote the exchange of the most up-to-date knowledge. That approach provided law enforcement officers in Member States with the tactical and operational planning advice necessary to make a real impact at the local, regional and international levels.

13. In the Middle East and North Africa, under a regional project on supporting regional capacities to prevent and combat cybercrime and implement digital forensics, UNODC cybercrime mentors based in Cairo continued to support Algeria, Egypt, Jordan, Lebanon, Libya, Morocco, the Sudan, Tunisia and the State of Palestine through activities that included:

(a) The conduct, in collaboration with national and international experts, of a comprehensive review to identify the legal provisions governing the prevention of and fight against cybercrime, including secondary legislation, rules and directives;

(b) The expansion of existing UNODC training material and expertise, and the development and delivery of training modules for forensic law enforcement personnel on electronic evidence collection;

(c) The conduct, in selected States, of assessments of the current level of public awareness and reporting of cybercrime;

(d) The delivery of technical advice on the establishment of a system of focal points for mutual legal assistance and extradition services at the ministries of justice of selected countries;

(e) The procurement and delivery of digital forensic triage equipment.

14. Moreover, in order to deliver capacity-building and technical support based on identified needs, UNODC conducted, upon request, comprehensive assessments of law enforcement and judicial cybercrime capabilities in Costa Rica, Pakistan, Peru and Uganda. The authorities of those countries were provided with the assessment reports that contained recommendations for supporting the development and implementation of specific policies and measures to counter cybercrime. In Costa Rica, on the basis of the UNODC assessment, the Attorney General's Office began considering the establishment of a specialized cybercrime unit. In addition, training needs for law enforcement and criminal justice practitioners in Costa Rica have been identified and capacity-building activities planned for 2020.

15. Each State member of ASEAN has, with the support of UNODC, created a mechanism for integrated national coordination, cooperation and information exchange on cybercrime matters, entitled the National Cybercrime Roundtable Discussion. The mechanism was designed to assist relevant national authorities in cooperating and in fostering intra-agency cooperation on cybercrime, digital forensics and cryptocurrencies. In this way UNODC is helping to bring together relevant government and private industry entities to discuss current cybersecurity, cybercrime and digital forensics challenges and issues, as well as what each entity could do better to address them. The Discussion acts as a forum for the exchange of information and good practice, and provides UNODC with the necessary information to develop its cybercrime technical assistance programmes nationally and across the greater South-East Asia region.

### Cybercrime investigations and digital forensics

16. In its resolution 74/173, the General Assembly encouraged Member States to develop and implement measures to ensure that cybercrime and crimes in which electronic evidence is relevant could be effectively investigated and prosecuted at the national level and that effective international cooperation could be obtained in that area, in accordance with domestic law and consistent with relevant and applicable international law, including applicable international human rights instruments.

17. In the same resolution, the General Assembly urged Member States to encourage the training of law enforcement officers, investigative authorities, prosecutors and judges in the field of cybercrime, including in relevant skills in evidence collection and information technology, and to equip them to effectively carry out their respective roles in investigating, prosecuting and adjudicating cybercrime offences.

18. During the reporting period, UNODC trained 1,817 criminal justice practitioners from 36 countries in the following areas: measures to counter online child sexual exploitation; use of specialized hardware and software; handling of digital evidence, digital forensic analysis; use of open-source intelligence tools; international cooperation; cybercrime law; intelligence on cyberthreats; cryptocurrency; darknet investigations; online investigations into wildlife crime; cyberthreat intelligence in countering terrorist operations; and malware investigations.

19. As part of that training, approximately 85 law enforcement officers from Eritrea, Ethiopia, Kenya, Uganda and the United Republic of Tanzania were trained in the use of digital evidence and online investigation techniques. Jointly with INTERPOL, UNODC also trained 19 police officers from across Africa in advanced malware investigation techniques. In Kenya, specialized digital forensic equipment, as well as mentoring support, have been provided to police officers in relation to digital forensics and triage techniques. That equipment and support help officers to focus on

the most salient evidence and have the greatest possible impact using minimal resources. Furthermore, UNODC, in cooperation with INTERPOL and the East African Police Chiefs Cooperation Organization (EAPCCO), commenced the development of the EAPCCO cybercrime investigation handbook.

20. In Central America, in cooperation with the Department of Justice of the United States of America and the National Judiciary Council of El Salvador, UNODC trained more than 200 Salvadoran judges in cybercrime and electronic evidence and developed guidelines for judges on the admissibility of digital evidence in court. Moreover, prosecutors, investigators and digital forensic analysts in Latin America enhanced their capacities in open-source intelligence, obtaining electronic evidence across borders, and in other aspects of cybercrime investigation and prosecution. Equipment to shield against remote interference was provided to the Cybercrime Unit of the National Civil Police of El Salvador, thus supporting the ability of the Government to promote good governance and the rule of law. In Guatemala, two regional technical assistance units (digital forensic laboratories) of the Directorate of Criminal Investigations of the Attorney General's Office were established, equipped and trained, enabling the Office to carry out prompt and effective investigations. Previously, the institutional response time was up to two months; following the establishment of the units, that response time fell to less than ten days.

21. In South-East Asia, trainers from five ASEAN member States (Indonesia, Malaysia, the Philippines, Thailand and Viet Nam) received training in cybercrime investigation to enable them to design and deliver training programmes in their law enforcement and criminal justice institutions. In the Lao People's Democratic Republic, UNODC assisted the police force in establishing and training the personnel of the first ever digital forensic laboratory. That directly ensured that the State was no longer a jurisdiction of risk for cyber-dependent and cyber-enabled crime, as it gave the authorities the ability to respond to those threats across all crime and terrorism typologies, within a broad human rights-based framework. In that manner, UNODC assisted in enhancing international cooperation and reducing threats. Furthermore, public-private partnerships were fostered across Asia through ministerial-level speaking events held in China, particularly at the World Internet Conference. That created the conditions for easier, more effective collaboration between law enforcement and technology firms to ensure the effective and timely preservation and delivery of digital evidence.

**Cryptocurrencies and darknet investigations**

22. During the reporting period, UNODC provided advice on cryptocurrency crime policy for Governments, and in support of the work of the Financial Action Task Force on virtual assets. UNODC e-learning tools are helping to improve policymakers' understanding of the threat and the need for a cohesive policy response, which is particularly important in view of the increase in cryptocurrency-facilitated crime, terrorism and probable State-aligned proliferation activities.

23. At the regional level, South-East Asia has continued to enhance the capacities of cryptocurrency investigative practitioners through the UNODC train-the-trainers approach. That approach has increased Member States' awareness of the threat and contributed to the development of cohesive law enforcement response capability. ASEAN countries, under the guidance of UNODC, are analysing national frameworks and legislation on cryptocurrencies and their potential use in money-laundering, terrorist financing and other criminal activities. The process has led Thailand to draft new regulations on the use of cryptocurrencies and the operation of cryptocurrency exchanges.

24. Authorities in ASEAN member States have also started to create and strengthen cryptocurrency investigation units to trace and seize cryptocurrency assets. For example, as a direct result of capacity-building provided by UNODC, the Malaysian Cryptocurrency Investigation Unit increased its personnel from two to sixteen

investigators – thus enabling long-term, self-sustained strategic organizational improvements. Two other ASEAN countries are in the process of creating such units and are benefiting from UNODC mentoring during the process.

25. In addition, law enforcement guidelines for seizing cryptocurrencies have been drafted by a working group on cryptocurrency comprising experts from ASEAN countries, international organizations and private companies. The guidelines, which are available only to verified criminal justice actors, are flexible and responsive to the evolution of the cryptocurrency marketplace.

26. In 2019, more than 200 officers from law enforcement agencies, central bank authorities, financial intelligence units and prosecutor's offices in South-East Asia and China received hands-on training in cryptocurrency and darknet investigations. UNODC tactical advice, requested as a direct result of cryptocurrency investigative training, supported responses to a number of kidnap cases in South-East Asia.

### Online child sexual abuse and exploitation

27. In its resolution 74/174, the General Assembly requested UNODC to assist Member States, upon request, in developing and implementing measures to increase access to justice and protection, including through domestic legislative and other measures for victims of child sexual exploitation and sexual abuse online, bearing in mind child- and gender-sensitive procedures, to obtain a just and timely remedy for violations of their rights. It also encouraged Member States to contribute resources to UNODC, including the Global Programme on Cybercrime, in order to counter child sexual exploitation and sexual abuse online.

28. In Kenya, the UNODC cybercrime mentor provided regular mentoring sessions at the Anti Human Trafficking, Child Protection Unit of the Directorate of Criminal Investigations. The training focused on electronic evidence and digital forensics. UNODC has also supported Operation Safisha, launched by the Unit to target online child abuse.

29. In Latin America, in partnership with INTERPOL and the International Centre for Missing and Exploited Children, UNODC trained more than 250 criminal justice practitioners in Barbados, Belize, Chile, Costa Rica, El Salvador, Honduras, Panama and Peru in the investigation of online child sexual exploitation. Non-governmental organizations working in the area of the promotion and protection of children's rights in Costa Rica were taught about the way cybercriminals use information and communications technologies to groom and, ultimately, sexually abuse and exploit children. As a result of a sustained dialogue supported by UNODC between the Costa Rican authorities, the International Centre for Missing and Exploited Children and Facebook, the Government committed to taking action in order to implement the Cybertip mechanism, supported by the National Centre for Missing and Exploited Children, to report online child sexual abuse and exploitation. In Belize, UNODC engaged with the authorities to advocate for amendments to the criminal code to criminalize cyber-facilitated crimes against women and children.

30. Moreover, also in Latin America, a victim identification task force was established in collaboration with INTERPOL. Eleven countries (Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Mexico and Peru) worked together to identify 66 children and 14 offenders through the effective use of the International Child Sexual Exploitation database.

31. In South-East Asia, UNODC supported six countries (Cambodia, the Lao People's Democratic Republic, Malaysia, Myanmar, Thailand and Viet Nam) in enhancing national multisectoral responses in order to prevent and tackle online child sexual exploitation and abuse.

### The use of the Internet for terrorist purposes

32. The use of the Internet for terrorist purposes remains one of the criminal activities that poses the most significant difficulties to criminal justice practitioners

and investigators in the commencement and conduct of investigations and subsequent prosecutions.

33. UNODC has helped Member States in that regard by designing and leading regional exercises on cyberthreat intelligence collaboration for joint cybercrime and counter-terrorism responses, which have strengthened synergies on cyber-related matters at the national and international levels.

34. As a result of joint training exercises between UNODC, INTERPOL and the European Union, with the participation of several private sector partners, some 60 front-line practitioners from 12 East African countries were trained in the use of open-source intelligence techniques to investigate the aftermath of terrorist events. The events also provided opportunities for criminal justice practitioners to forge informal alliances with their regional counterparts.

35. Approximately 40 financial investigators, law enforcement officers and non-profit organization representatives in Mauritius received training on the relationship between social media and the radicalization and infiltration of non-profit organizations by terror groups.

36. At the request of the Anti-Terror Police Unit of Kenya and as a part of continuous mentoring efforts, a UNODC cybercrime mentor assisted in the investigation into the aftermath of the Dusit Hotel attack by providing equipment and operational advice to enable more efficient examination of the digital devices that had been seized.

37. In South and South-East Asia, more than 200 criminal justice practitioners enhanced their capacities for preventing and investigating cyberattacks by terrorist actors. They were trained in how to gather, search and analyse open-source intelligence and to track down organized criminal groups and terrorists on the darknet, as well as in other specialized cyberinvestigation techniques.

**International cooperation to obtain electronic evidence**

38. On 10 and 11 December 2019, within the framework of the global initiative entitled “Strengthening the capacity of central authorities and counter-terrorism prosecutors and investigators in obtaining digital evidence from private CSPs in cross-border investigations, with a particular focus on counter-terrorism matters”, UNODC, the Counter-Terrorism Committee Executive Directorate and the International Association of Prosecutors jointly organized a specialist workshop, held in in Washington, D.C., on obtaining electronic evidence through mutual legal assistance. Dedicated entirely to the topic of obtaining electronic evidence through mutual legal assistance mechanisms, the workshop used as reference material the *Practical Guide for Requesting Electronic Evidence Across Borders*, released in 2019. The workshop offered an opportunity for practitioners (including liaison magistrates to the United States, national prosecutors and representatives of central authorities, representatives of the United States Department of Justice and technical experts) to discuss the practical aspects of cooperation and ongoing challenges, as well as identify and share good practices to strengthen the expeditious processing of requests for mutual legal assistance with the United States, with a view to enhancing the effectiveness of the investigation and prosecution of terrorism and other serious crimes around the world.

# IV. Information-sharing

39. In its resolution 74/173, the General Assembly reaffirmed the role of UNODC, pursuant to Commission on Crime Prevention and Criminal Justice resolution 22/8 of 26 April 2013, as a central repository of cybercrime laws and lessons learned with a view to facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.

40. In 2019, UNODC continued to work on including cybercrime-related resources in the Sharing Electronic Resources and Laws on Crime knowledge management portal. As of January 2020, the portal contained more than 1,300 pieces of legislation on cybercrime and 39 cyber-enabled or cyber-dependant cases, illustrating the links between cybercrime and other types of crime such as participation in an organized criminal group, money-laundering and drug trafficking.

41. UNODC also continued to use social media to share cyber-related information and significantly increase the public visibility of its work. That led to more than 2.8 million Twitter impressions and increased recognition of the Office's work.

# V. Research and analysis

42. In 2019, UNODC commenced research on darknet-based threats in South-East Asia. That work continued in 2020; the Office will be able to provide further information in that regard by the end of the year.

# VI. Prevention

43. The start of 2019 saw the finalization of a series of university modules on cybercrime[1] – the result of collaborative work by leading experts and academics from over 25 countries in six different continents, as well as INTERPOL and the Office of the United Nations High Commissioner for Human Rights. The series, which was developed under the Education for Justice initiative of the UNODC Global Programme for the Implementation of the Doha Declaration, consists of a teaching guide and 14 modules. At the workshops organized by UNODC to promote the use of the series of university modules on cybercrime, university professors from Africa, Europe and West and Central Asia enhanced their familiarity with the series and learned how to adapt and integrate the modules into existing or new courses. UNODC thereby equipped professors at 40 universities in 25 countries in five continents to build comprehensive, cross-discipline courses on cybercrime in the academic year 2019/20. As a result, more than 7,200 students around the globe have been taught about various aspects of cybercrime on the basis of the UNODC series. An understanding of key issues related to cybercrime will help young people, who are future policymakers, criminal justice practitioners and information technology specialists, to develop efficient solutions to make both the online and offline worlds safer from crime.

44. UNODC, under its Education for Justice initiative and in cooperation with leading education experts, developed innovative learning tools, including animated videos, computer and non-electronic games and comic books, on topics such as online safety and cybercrime for use in primary and secondary schools. The animated videos and comic books are supplemented by a teacher's manual and lesson plans to enable teachers to use the tools in their classes. Throughout the year, UNODC raised cybercrime awareness among the public, practitioners and decision makers worldwide, through the proactive use of social media, attracting several million impressions and interactions. The Global Programme on Cybercrime has 8,110 followers and, with an average of 220 tweets per month, has achieved 2.5 million Twitter impressions, which have directly resulted in members of the public seeking advice after becoming victims of cybercrime, or noting their appreciation for the work of UNODC to counter cybercrime. United Nations resident coordinators, diplomats and authorities from Member States have contacted UNODC to seek advice and information regarding the politics related to cybercrime.

45. In Guatemala and El Salvador, UNODC supported the ministries of education in designing, adopting and implementing a prevention strategy on cybercrime at public schools. The strategy included specialized training on cybercrime prevention

[1] Available at www.unodc.org/e4j/en/tertiary/cybercrime.html.

for an awareness campaign, and the designing of two guidelines for teachers on how to teach cybercrime prevention. Both ministries introduced actions to prevent cybercrime into their regular activities, targeting not only students but also teachers. The Ministry of Education of El Salvador reported that the strategy had had an impact on 3,222 teachers, 37,361 students and 12,511 parents, while in Guatemala, it had reportedly had an impact on 188,477 students and 9,042 teachers.

46. Permanent exhibitions on cybercrime were designed, built and launched at the children's museums of Guatemala and El Salvador. Developed in coordination with the Education for Justice initiative, the exhibitions were designed to promote and provide information on the rights of children on the Internet, through a series of 10 rights and duties relating to information and communications technologies and through a virtual reality game that stressed the importance of a responsible approach to the access and use of information and communications technologies for informative and recreational purposes. Partnerships with private companies such as Telefonica, and with the non-profit organization Fundación Azteca and a radio station, were established in order to promote cybercrime prevention in El Salvador and Guatemala.

# VII. Expert Group to Conduct a Comprehensive Study on Cybercrime

47. UNODC supports, through its substantive and secretariat functions, the work of the Expert Group to Conduct a Comprehensive Study on 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 propose new national and international legal and other responses to cybercrime. The Expert Group was established by the Commission on Crime Prevention and Criminal Justice in accordance with General Assembly resolution 65/230, in which the Assembly endorsed the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, adopted at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. The Expert Group's 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 Nations Congress on Crime Prevention and Criminal Justice and endorsed by the General Assembly in its resolution 70/174.

48. The Expert Group has held a total of five meetings, in 2011, 2013, 2017, 2018 and 2019. Its sixth meeting is to be held from 6 to 8 April 2020. In its resolution 26/4, the Commission on Crime Prevention and Criminal Justice requested the Expert Group to continue its work. This work, to be conducted on the basis of a structured workplan, is aimed at compiling recommendations to be considered at a stock-taking meeting to be held no later than 2021, with a view to producing a consolidated and comprehensive list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.

49. The fifth meeting of the Expert Group was held from 27 to 29 March 2019, and focused on law enforcement, investigation, electronic evidence and criminal justice. At the meeting, the Expert Group was informed about successful national efforts to implement legal and procedural measures to tackle cybercrime; develop and implement cybersecurity strategies and policies; enact and upgrade legislation on cybercrime; implement new investigative tools to gather electronic evidence and establish its authenticity for evidentiary purposes in criminal proceedings; and implement institutional arrangements for the more efficient use of resources to combat cybercrime. The need for appropriate procedural powers to obtain electronic evidence was highlighted, as were challenges arising from conflicts regarding

territorial jurisdiction. The discussion also focused on how to strike a balance between the need for effective law enforcement responses to cybercrime and the protection of fundamental human rights, in particular, the right to privacy. The Expert Group accorded priority to the need for sustainable capacity-building within national law enforcement and criminal justice systems as a prerequisite for enhancing domestic capabilities and for enabling the sharing of good investigative practices and experience and the dissemination of new techniques.

50. In its resolution 74/173, the General Assembly, inter alia, acknowledged the importance of the work of the Expert Group to continue to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime; noted with appreciation that the Expert Group would develop, in accordance with its workplan for the period of 2018–2021, possible conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice; recognized the Expert Group as an important platform for the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses for cybercrime; requested the United Nations Office on Drugs and Crime to continue to periodically collect information on new developments, progress made and best practices identified and to periodically report that information to the Expert Group and the Commission; and invited the Expert Group to provide advice, on the basis of its work, to the United Nations Office on Drugs and Crime, including with regard to the Global Programme on Cybercrime, in order to assist, without prejudice to other issues included in the mandate of the Expert Group, in identifying high-priority capacity-building needs and effective responses, without prejudice to the status of the Commission as the governing body of the crime programme of the Office.