United Nations E/CN.15/2021/13

Economic and Social Council

Distr.: General
8 March 2021

Original: English

Commission on Crime Prevention and Criminal Justice
Thirtieth session
Vienna, 17–21 May 2021
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 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. As the twenty-ninth session had to be held in a scaled-down format, owing to the coronavirus disease (COVID-19) pandemic, the report is being made available to the Commission at its thirtieth session.

The report describes progress made in 2020 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.15/2021/1.

I. Introduction

United Nations Office on Drugs and Crime cybercrime mandates

1. In 2009, in its resolution 64/179, 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. 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 could facilitate that activity.

II. New developments, progress made and best practices identified

6. Cybercrime evolved during the coronavirus disease (COVID-19) pandemic and throughout 2020, resulting in new challenges with a global impact. Criminals took advantage of the desire for information, support and reassurance. Health care was compromised through phishing campaigns related to COVID-19 and the targeting of hospitals with ransomware.

7. In response to the above mandates and global developments, UNODC – primarily through its Global Programme on Cybercrime – provided technical assistance and capacity-building on cybercrime to Member States at the national, regional and global levels. UNODC also functions as the secretariat to the Expert Group to Conduct a Comprehensive Study on Cybercrime.

8. In planning and implementing its counter-cybercrime activities, UNODC closely cooperates with and advises key cybercrime partners and forums such as the International Criminal Police Organization (INTERPOL), the International

Telecommunication Union (ITU), the European Union Agency for Law Enforcement Cooperation (Europol), the European Cybercrime Training and Education Group, the World Bank, the United Nations Children's Fund (UNICEF), the Association of Southeast Asian Nations (ASEAN), End Violence against Children and the Global Forum on Cyber Expertise. During the reporting period, UNODC continued to support the work of the General Assembly and contributed to the Secretary-General's Road Map for Digital Cooperation. Furthermore, the Office routinely provided guidance and advice on the impact of cybercrime on cybersecurity, peace and stability to senior United Nations officials, Member States and civil society.

9. During the reporting period, UNODC helped Member States to prevent, detect, investigate and prosecute cybercrime in all its forms, with due regard to human rights and fundamental freedoms. This included sharing actionable information to counter a specific COVID-19 fraud threat. UNODC also provided information to United Nations agencies to mitigate the cyber-based targeting of those agencies.

10. UNODC followed the developments relating to the adoption and implementation of General Assembly resolution 74/247, on countering the use of information and communications technologies for criminal purposes, which, among others, includes a mandate for the establishment of an open-ended ad-hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the Expert Group to Conduct a Comprehensive Study on Cybercrime (for information on the work of the Expert Group, see chapter VII below).

11. Also in that resolution, the General Assembly decided that the ad hoc committee should convene a three-day organizational session in August 2020, in New York, in order to agree on an outline and modalities for its further activities, to be submitted to the Assembly at its seventy-fifth session for its consideration and approval. Owing to the impact of the COVID-19 pandemic, the Assembly decided, in its decision 74/567, to postpone the organizational session to a date as early as conditions would permit, but not later than 1 March 2021. On 1 October 2020, Member States were informed that, in line with the requirements contained in Assembly decision 74/567, the dates of 20–22 January 2021 had been allocated to the organizational session of the Committee, which was to be held in New York.

12. Pursuant to General Assembly decision 75/555, entitled Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, the organizational session of the Ad Hoc Committee was postponed from 20–22 January to 10–12 May 2021. UNODC will provide technical and substantive support to and serve as the technical and substantive secretariat of the Committee. UNODC has prepared a background paper containing a proposed outline and modalities for the further activities of the Committee and has collected and disseminated comments from Member States on the proposed outline and modalities.[1] The Office has also organized several informal briefings to facilitate the consultations by Member States on the preparation for the organizational session.

III. Normative and capacity-building support

13. Cybercrime mentors based in Austria, El Salvador, Guatemala, Senegal and Thailand continued supporting countries in the corresponding regions to counter cyber-dependent and cyber-enabled crime and to handle and exchange electronic evidence. Moreover, in 2020, UNODC capacity-building continued to address the

[1] Available at www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html.

needs of developing countries. Owing to the COVID-19 pandemic, in March 2020, the operating model of the Global Programme on Cybercrime changed to full remote operations. Despite this, the programme continued to provide political, policy, strategic, tactical and operational advice, focused on Member States' self-identified pandemic-related vulnerabilities and challenges. This approach provided law enforcement officers in Member States with the tactical and operational-planning advice needed to have a real impact on local, regional and international casework, despite the difficulties related to COVID-19 faced by the officers themselves.

14. UNODC conducted, upon request, comprehensive assessments of law enforcement and judicial counter-cybercrime capabilities in Burkina Faso. In Belize, UNODC is supporting the drafting of a strategy and standard operating procedures to strengthen the cybercrime investigation capabilities of the police.

Cybercrime investigations and digital forensics

15. 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.

16. 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.

17. During the reporting period, UNODC trained 2,440 criminal justice practitioners from 64 countries on countering online child sexual exploitation and abuse, the use of specialized hardware and software, the handling of digital evidence, digital forensic analysis, the use of open source intelligence tools, international cooperation, cybercrime law, threat intelligence, cryptocurrencies, darknet investigations, wildlife crime online investigations, malware investigation, mobile forensics, due process and digital evidence, and cybercrime incident response. At the heart of this work are the human rights and fundamental freedom concepts of legality, necessity, proportionality and accountability.

Cryptocurrencies and darknet investigations

18. In the South-East Asian region, investigative cryptocurrency practitioners enhanced their capacities through the UNODC train-the-trainer approach. Support to the region raised the awareness of Member States about threats and developed a cohesive law enforcement response capability. UNODC delivered timely and relevant technical assistance and mentoring, such as through the provision of operational advice to a Member State regarding a complex criminal investigation involving cryptocurrencies. In 2020, more than 130 law enforcement, central bank and financial intelligence unit officials in Asia received hands-on training in cryptocurrency and darknet investigations, thus delivering strategic capacity supported by UNODC specialist mentoring.

19. During the reporting period, the third South-East Asia cryptocurrencies working group meeting was held. It was organized as part of an ongoing collaborative effort among South-East Asian countries to promote long-term and sustainable international cooperation on cybercrime and cryptocurrencies. The working group advocated for the reform of anti-money-laundering and combating the financing of terrorism frameworks and cryptocurrency regulations in line with the Financial Action Task Force guidance on virtual assets.

Online child sexual exploitation and abuse

20. 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 online child sexual exploitation and abuse, bearing in mind child- and gender-sensitive procedures, to obtain a just and timely remedy for violations of their rights. In the same vein, the Assembly encouraged Member States to contribute resources to UNODC, including the Global Programme on Cybercrime, in order to counter online child sexual exploitation and abuse.

21. The COVID-19 pandemic and the associated requirement to work and study from home has exacerbated online child sexual exploitation and abuse. The availability of a vastly increased victim pool, with more children being online with limited supervision, created new opportunities for abusers. As an example, in Central America, most cybercrime unit cases are related to online child sexual exploitation and abuse and crimes against women and girls. In El Salvador, during the period 2018–2020, 40 per cent of the 263 cases managed by the Cybercrime Unit involved online child sexual exploitation and abuse, while 32 per cent of cases involved the online sexual exploitation and abuse of women. By 2020, more than 50 per cent of cases involved investigations into online child sexual exploitation and abuse. In Honduras, during 2020, 7 out of every 10 child victims of online child sexual exploitation and abuse were girls. In Belize in 2019, the Cybercrime Unit investigated 39 cases involving sexual and financial crime; 85 per cent of them involved online child sexual exploitation and abuse. During 2020, although the number of investigations was lower, abuse reported by technology companies through the UNODC-supported reporting mechanism established in February 2020 showed an increase in the number of cases of online child sexual exploitation and abuse in Belize during COVID-19. The experience in Belize shows the necessity and effectiveness of having concurrent non-criminal justice responses to serious crime.

22. As a response, a series of webinars on online child sexual exploitation and abuse were delivered, in English, French, Portuguese and Spanish, across multiple time zones, to cover West Africa, Latin America and the Caribbean. During the webinars, 7,832 people (law enforcement officials, prosecutors, academics, representatives of non-governmental organizations and members of the general public) from 15 countries learned about cybercrime reporting mechanisms, technology initiatives, risks and challenges.

23. Furthermore, UNODC, in coordination with the International Centre for Missing and Exploited Children, designed a 12-week online diploma course, in English and Spanish, on online child sexual exploitation and abuse, which was delivered to 1,000 criminal justice practitioners from 44 countries.

24. In South-East Asia, UNODC organized the ASEAN Regional Conference on Child Online Protection, in coordination with UNICEF and ITU. The conference brought together representatives from the justice sector, ministries of telecommunications and education and non-governmental organizations and industry experts to discuss and raise awareness about existing and emerging online risks for children. The conference represented the continuation of UNODC efforts to maintain a platform for relevant agencies in the ASEAN region to discuss trends and challenges and design regulatory frameworks and investigative responses.

25. In Central America, and in coordination with ministries of education and trafficking in persons secretariats of El Salvador, Guatemala and Honduras, UNODC trained more than 5,600 teachers on cybercrime prevention, with an emphasis on the prevention of online child sexual exploitation and abuse. As a direct result of the training, 13 female victims of online child sexual exploitation and abuse (aged 9 to 12) were detected and safeguarded. The work brought together whole-of-government prevention, investigation, prosecution and adjudication skillsets, leading to better, evidence-based policy formulation by Governments.

26. Also in Central America, UNODC and the National Centre for Missing and Exploited Children worked with Costa Rica, El Salvador, Guatemala and Honduras to grant direct access for those countries to the Centre's case management tool. The tool is a platform that reduces bureaucracy when reporting cases of online child sexual exploitation and abuse detected by Internet service and social media providers based in the United States of America. The new model will ensure a victim-oriented operational framework, given that time is of the utmost importance in cases of online child sexual exploitation and abuse.

International cooperation to obtain electronic evidence

27. UNODC worked with global technology companies to provide training to criminal justice authorities on how to request digital evidence from them, with a special emphasis on online child sexual exploitation and abuse. The training programme created an environment for practitioners and representatives of the private sector to discuss policies, procedures and jurisdictional matters with companies including Facebook, Instagram, Microsoft and WhatsApp. A total of 655 justice practitioners from Belize, Costa Rica, El Salvador, Guatemala and Honduras benefited from the initiative.

IV. Information-sharing

28. 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, 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.

29. In 2020, UNODC continued including cybercrime-related resources into the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal. As of December 2020, SHERLOC contained more than 1,500 pieces of legislation on cybercrime and information on 42 cases of cyber-enabled or cyber-dependent crime, illustrating the linkages between cybercrime and other crime types, such as participation in an organized criminal group, money-laundering and drug trafficking.

30. UNODC uses social media to share cyber-related information in order to raise awareness and encourage prevention among the general public. This has led to over 2.8 million impressions on Twitter and LinkedIn. This work was further enhanced through profiling of the work of UNODC on television, radio, the Internet and the United Nations "Awake at night" podcast.

V. Research and analysis

31. In 2020, UNODC published *Darknet Cybercrime Threat Assessment for South-East Asia*. The report contains an assessment of the darknet from the user, criminal and law enforcement perspectives, with a particular focus on cybercriminality targeting South-East Asia.

VI. Prevention

32. To combat the increased prevalence of cybercrime threats owing to the COVID-19 pandemic, UNODC supported various prevention measures. Hosting its training online allowed UNODC to reach and raise the awareness of more teachers, students, children and parents with regard to cybercrime prevention. Online delivery also created the opportunity to increase the understanding of more officials from institutions and Governments of cybercrime, the importance of cybersecurity and the

use of technologies for committing crime. Awareness-raising was provided to more than 24,400 persons in South-East Asia, Africa and Latin America.

33. Also in South-East Asia, Africa and Latin America, UNODC launched cybercrime prevention campaigns on social media and television aimed at children and students. In Africa, a prevention campaign was launched on social media in English, French and Portuguese. In El Salvador and Guatemala, prevention campaigns were launched on national television. In Guatemala, the campaign was launched in partnership with Television Azteca and was called “The Internet in times of lockdown”. The campaign received 28.5 million views.

34. During the COVID-19 pandemic, schools were often closed and had to migrate to online classrooms. In El Salvador, UNODC designed a protocol on cyber-incident response for online classes and trained 650 information technology staff and teachers.

VII. Expert Group to Conduct a Comprehensive Study on Cybercrime

35. UNODC supports, through its substantive and secretariat functions, the work of the Expert Group to Conduct a Comprehensive Study on Cybercrime. The Expert Group examines cybercrime and responses to it by Member States, the international community and the private sector. This includes 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. The Group was established by the Commission on Crime Prevention and Criminal Justice in accordance with General Assembly resolution 65/230, in which the Assembly had endorsed the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, adopted by the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. The aforementioned 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.

36. The Expert Group has held a total of six meetings, in 2011, 2013, 2017, 2018, 2019 and 2020. In its resolution 26/4, the Commission on Crime Prevention and Criminal Justice requested the Expert Group to continue its work, decided that the Group would dedicate its future meetings to examining, in a structured manner, each of the main issues dealt with in chapters three through eight of the study and encouraged the Group to develop possible conclusions and recommendations for submission to the Commission. The stocktaking meeting, the seventh meeting of the Group, is to be held from 6 to 8 April 2021.

37. The sixth meeting of the Expert Group was scheduled to be held from 6 to 8 April 2020, but it had to be postponed owing to the COVID-19 pandemic. Upon approval by the extended Bureau, it was held from 27 to 29 July 2020, with the Chair and representatives of the secretariat present in the meeting room and all other participants attending online, with simultaneous interpretation provided through an online platform. At that meeting, the Expert Group focused on international cooperation and prevention of cybercrime. Again, diverse views were expressed in relation to whether a new universal or global legal instrument on cybercrime was needed within the framework of the United Nations. The Group was informed that, since its previous meeting, there had been developments that led to the adoption by the General Assembly of resolution 74/247, in which the Assembly had decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention

on countering the use of information and communications technologies for criminal purposes (see above).

38. At that meeting, the expeditious execution of mutual legal assistance requests was identified as one of the most important conditions for effective measures against cybercrime and other offences involving electronic evidence. Emphasis was placed on the significance of networking for enhancing international cooperation to address cybercrime. Furthermore, the Group discussed cybercrime prevention as an important component of national policies and strategies to address challenges posed by cybercrime. Multi-stakeholder cybercrime strategies were widely identified as a vital preventive element in the fight against cybercrime.

39. Given the challenges of Internet connectivity and the reduced duration of the meetings as a result of the new meeting format, a list of preliminary recommendations and conclusions as compiled by the Rapporteur on the basis of the discussions and deliberations during the meeting was included in the report on the meeting (UNODC/CCPCJ/EG.4/2020/2). Those preliminary recommendations and conclusions, together with the conclusions and recommendations resulting from the meetings of the Group held in 2018 and 2019, will be further discussed at the seventh meeting, to be held from 6 to 8 April 2021, in order to produce a consolidated and comprehensive list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.