3 April 2017

English only

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 10-13 April 2017

Information on the implementation of Crime Commission resolution 22/8

Note by the Secretariat

I. Introduction

1. In its resolution 22/8, entitled "Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime", the Commission on Crime Prevention and Criminal Justice invited the United Nations Office on Drugs and Crime (UNODC), in close cooperation with Member States, to advance the implementation of the Global Programme on Cybercrime.

2. In the same resolution, the Crime Commission requested UNODC, on the basis of the needs of requesting States, to strengthen partnerships for technical assistance and capacity-building to counter cybercrime with Member States, relevant organizations, the private sector and civil society.

3. Furthermore, in resolution 22/8, the Crime Commission requested UNODC to serve as a central data 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.

4. The Crime Commission, in its resolution 22/8, invited Member States and other donors to provide extrabudgetary resources, where necessary and in accordance with the rules and procedures of the United Nations, for the implementation of the resolution.

5. Also in resolution 22/8, the Crime Commission requested the Executive Director of UNODC to submit a report to the Commission at its twenty-third session on the implementation of the resolution and the work of the Global Programme on Cybercrime. Since the required extrabudgetary resources were not made available to the Secretariat, a report for the twenty-third session of the Crime Commission was not produced.[1]

[1] For further information, see the Annotated provisional agenda for the twenty-third session of the Crime Commission (E/CN.15/2014/1) and the Statements of financial implications presented to the Commission on Crime Prevention and Criminal Justice before its consideration of draft resolutions at its twenty-second session (E/CN.15/2013/CRP.10).

6. The present note by the Secretariat contains information regarding the implementation of Crime Commission resolution 22/8 and has been prepared for the third session of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime.

II. The Global Programme on Cybercrime

7. The objective of the UNODC Global Programme on Cybercrime is to respond to identified needs in developing countries by supporting Member States to prevent and combat cybercrime in a holistic manner through the delivery of crime prevention and criminal justice technical support, based on UNODC assessment protocols and technical assistance tools.

8. Since commencing in January 2013, the Programme has delivered a broad range of services to over 50 Member States in Central America, Eastern Africa and South-East Asia, as well as to other regions from its headquarters Vienna. The focus of the deliverables of the Programme includes:

(a) Increased efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime — especially online child sexual exploitation and abuse — within a strong human-rights framework;

(b) Efficient and effective long-term whole-of-government response to cybercrime, including national coordination, data collection and effective legal frameworks, leading to a sustainable response and greater deterrence;

(c) Strengthened national and international communication between government, law enforcement and private sector with increased public knowledge of cybercrime risks.

9. The Programme now has an impact and scope beyond its relatively small funding position and limited number of staff. The relevance of cybercrime as a thematic priority continues to grow across the globe and UNODC will continue to offer its specialized capabilities to address the threat, in conjunction with international partners and Member States.

A. Technical assistance and capacity-building activities

10. In 2013 and 2014, in Eastern Africa, the Programme carried out a number of cybercrime assessment missions, in conjunction with host governments, in order to identify main challenges, threats and the capability to respond. Based on these strategic analyses, digital forensic evidence training courses were delivered by consultants in four countries. In South-East Asia, a similar approach was taken in nine countries, with UNODC's standardized Criminal Justice Assessment toolkit being used to assess (i) policing; (ii) access to justice; (iii) custodial and non-custodial measures; and (iv) cross-cutting issues. Subsequently, training courses on digital evidence techniques were delivered by a number of consultants.

11. In El Salvador, a more nuanced approach was taken to ensure that a whole-of-government response was developed. This included support to legal drafting and analysis, policy analysis, criminal justice assessments and advocacy and outreach. With sustainable staffing and funding, the work which commenced in El Salvador in 2014 has ensured a truly successful, cross-government counter-cybercrime capability.

12. In Central America, programme impact increased in 2015 as more countries joined the training and mentoring sessions delivered by UNODC. Common experiences and language and the desire to make a positive difference ensured that law enforcers, prosecutors and judges came together to address similar challenges, as well as to identify solutions and strengthen collaboration.

13. In Eastern Africa, a network of dedicated prosecutors, judges and criminal justice officials with cybercrime experience was created and expanded. In UNODC's experience, supporting the establishment and growth of such networks of officials within geographic regions helps sustain the outcomes of formal training by forging relationships and building trust, thereby increasing programme delivery.

14. In 2016, there was a significant growth in the Programme's reach, breadth and impact. Over 250 investigators, prosecutors and judges were trained to interpret digital evidence, conduct online investigations, cooperate with social networks and assess online crime scenes. Using the #WePROTECT Global Alliance Model National Response,[2] criminal justice professionals learned about some of the significant challenges in investigating online child sexual exploitation, and understood their personal roles in building a holistic cross-government response.

15. An increase in public outreach and advocacy led over 11,000 children, adults and caregivers to learn about online risks and be empowered to make better decisions online. With over 200 cybercrime investigations being mentored by UNODC, a more detailed picture of threats and vulnerability assessments were possible in the jurisdictions hosting staff of UNODC's Global Programme on Cybercrime.

16. While the loss of staff in Eastern Africa due to a lack of funding is regrettable, new funding sources made possible the growth of the Programme's work in Guatemala and via UNODC's Regional Programme in Tunisia. An unexpected increase in funding enabled the creation of a new specialist post in Bangkok (with the post having been filled in February 2017).

17. In summary, the key requirements with respect to technical assistance and capacity-building activities for 2016, to re-engage donors and recipients, build confidence and expand the Programme, were successfully concluded. Many other Member States continued to reach out to UNODC for assistance; however, due to a lack of funding, UNODC was unable to assist. Despite this, proactive investigations had tangible benefits on the lives of the public. The Programme delivered jointly with other UNODC Programmes[3] and the standing of UNODC as a partner of choice within the cybercrime ecosystem grew.

B. Partnerships for technical assistance and capacity-building to counter cybercrime

Collaboration with international organizations

18. Collaboration is at the core of the UNODC Global Programme on Cybercrime. New, mutually beneficial relationships were built with the International Centre for

[2] "At the Abu-Dhabi Summit in 2015, governments and organisations agreed to establish and deliver, in their own countries, a coordinated national response to online child sexual exploitation, guided by the WePROTECT Global Alliance Model National response (MNR). This document provides guidance and support on the MNR to countries and organisations to help them deliver on this commitment. Whilst the Model is focused on helping countries to build their response to online child sexual exploitation, it acknowledges that this cannot be addressed in isolation and a wider set of capabilities to prevent and tackle child sexual exploitation and abuse are required to be in place to ensure a complete national response." *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*, November 2016. More information is available at the WE Protect Global Alliance website: http://www.weprotect.org/the-model-national-response/.

[3] The Global Programme on Cybercrime has delivered capacity-building in 2016 jointly with the Global Programme Against Money-Laundering, Proceeds of Crime and the Financing of Terrorism (GPML), the Global Firearms Programme, the Global Programme to Support to the work of the Conference of the Parties to the UNTOC Convention, the Global Programme for Strengthening the Capacities of Member States to Prevent and Combat Organized and Serious Crimes and the Global Programme On Building Effective Networks Against Transnational Organized Crime (BENATOC).

Missing and Exploited Children (ICMEC), INTERPOL, Council of Europe, the Organization of American States, Europol, World Bank, the International Telecommunications Union, UNICEF, the Organization for Security and Cooperation in Europe, and others. The collaboration features regular coordination calls and sharing of resources as appropriate, which ensures that strategic capacity-building occurs with minimum duplication of efforts and maximum impact.

Collaboration with the private sector

19. In addition to strengthening connections with Communication Service Providers in the regions where the Programme is present, new relationships were built with online portals, social media services and other software providers such as Google, Facebook and Microsoft. This ensures that the most up-to-date techniques for accessing proportionate, legal, accountable and necessary digital evidence are delivered within a strong, transparent human rights framework.

Collaboration with civil society

20. Relationships were developed with ECPAT International[4] in Bangkok and the International Justice Mission in Sydney — both of whom bear relevance to the counter-child sexual exploitation narrative. The Programme has also engaged closely with Oxford University's Cyber Capacity Centre and the Netherlands-based Global Forum on Cyber Expertise.

C. Funding of the Global Programme on Cybercrime

21. As of January 2017, the Programme was funded through voluntary contributions from Australia, Canada, Japan, Norway, the United Kingdom of Great Britain and Northern Ireland and the United States of America. Two of these donors have revealed that, with regret, further funding in 2017 is unlikely.

22. The funding position of the Programme therefore remains challenging. The increased confidence in the Programme's activities for 2016 and 2017 ensured that donors kindly supported the growth of the Programme. However, at this time, there is little funding to continue after December 2017. UNODC urgently requests the continued assistance of donors — particularly in the form of crucial non-earmarked funds which can ensure the continued employment of our specialist counter-cybercrime mentors in Central America and South-East Asia.

23. A figure of approximately USD 3,000,000 per annum would ensure that the Programme has the necessary staff in place in Central America, Eastern Africa and South-East Asia, the means to deliver measureable impact in the Member States, and the capacity to respond to ad hoc requests that currently cannot be fulfilled due to lack of resources. The Global Programme on Cybercrime has measureable impact, saves lives and prevents the victimization of vulnerable sectors of society. The relevance of the Programme continues to grow along with the persistent increase in digital evidence and internet-based criminality on both the clearnet and the darknet.

24. UNODC wishes to continue to use its specialized capacities, law enforcement expertise, legislative assistance services and public outreach to play a leading role, with partners, in countering cybercrime around the world.

III. The Cybercrime Repository

25. The UNODC Cybercrime Repository was created in 2015 and was made possible through funding from the United Kingdom. Case law, legislation, best

[4] Non-profit organization that started as a campaign to End Child Prostitution in Asian Tourism. More information is available at the ECPAT International website: http://www.ecpat.org/.

practices and lessons learned continue to be included in the repository and analytic data show its use is growing, possibly in part due to the Programme's broader social media and public outreach.

26. However, there is no further funding anticipated for the maintenance and expansion of the repository, which makes continued technical support extremely challenging.