29 July 2020

English only

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 27–29 July 2020

Draft report

Addendum

II. List of preliminary recommendations and conclusions (*continued*)

B. Prevention

(1) Cybersecurity practices are distinct from efforts to combat cybercrime. States should develop both a national cybercrime strategy, including national legislation or policy for cybercrime prevention, and a national cybersecurity strategy. Focus areas for national cybercrime strategies should include cybercrime prevention, public-private partnerships, criminal justice capacity, and awareness raising through published court decisions.

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

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

(4) "Criminal justice capacity" should be another area of focus in national cybercrime strategies. Assistance to developing countries should be a priority in order to strengthen law enforcement capacity in preventing cybercrime.

(5) Member States should avail themselves of capacity-building assistance from the UNODC Global Program on Cybercrime and other initiatives, including the Council of Europe GLACY+ programmes.

(6) States should develop or strengthen support programmes for victims of cybercrime.

(7) States should undertake surveys to measure the impact of cybercrime on businesses, including measures implemented, employee training, types of cyber incidents that affect them and the costs associated with recovering from and preventing cyber incidents.

(8) States should support business and communities to raise awareness of cybercrime risks, mitigation strategies, and enhance cyber practices, as these can have significant downstream preventative benefits.

(9) The modus operandi of contemporary cybercriminals should be carefully studied by means of intelligence analysis and criminological research in order to deploy existing resources more effectively and identify vulnerabilities.

(10) States should consider setting up a coordination platform to promote the instant exchange of data on incidents and new trends in cybercrime that have been identified. States should also consider establishing criminological observatories to monitor cybercrime threats and trends.

(11) Countries should consider specific and tailored efforts to keep children safe online. This should include ensuring domestic legal frameworks, practical arrangements and international cooperation arrangements enable reporting, detection, investigation, prosecution and deterrence of child sexual abuse exploitation and abuse online.

(12) Industry is a key partner in preventing cybercrime. Countries should consider implementing mechanisms for cooperating with industry, including on referrals to competent national authorities and takedowns of harmful criminal material, including child sexual exploitation and abhorrent violent material.

(13) Regular advisories on incident prevention should be issued and shared with users and organizations/stakeholders to enable them to prevent cyber incidents that would potentially lead to criminal activities.

(14) There should be a methodology and standard procedures for sharing live information based on evidence to prevent cybercrimes.

(15) A mechanism should be developed to register all online services and to implement minimum baseline security standards through domestic regulation.

(16) States should consider using artificial intelligence to design systems that will automatically reconfigure themselves in the face of attacks.

(17) It was recommended that a global database on cryptocurrency abuses and the massive exploitation of criminal data should be created, as well as a globally coordinated strategic overview of the threats posed by criminal offences committed on the darknet.

(18) Regional and international initiatives aimed at strengthening cybersecurity should be encouraged, in particular by exchanging information on large-scale cyber attacks.

(19) States may consider establishing an international cyber threat information-sharing system to share and study the technologies as well as modus operandi of new threats.

(20) States are encouraged to establish a tiered cybersecurity protection system to adopt different information security technologies and management measures for different information and communication facilities, and to ensure that critical infrastructures are protected from cybercrime.

(21) States should involve female experts in the prevention and investigation of cybercrime.

(22) National and regional prevention experiences should be brought together to create a multilateral repository that would allow the dissemination of good practices in diverse contexts.

(23) Measures should be strengthened with the aim at preventing the spread of hate speech, extremism and racism.

(24) Greater awareness should be generated and legislative assistance should be provided on regulatory frameworks against cyberbullying and online violence.

(25) Capacity-building and cooperation should be provided for the prevention of cybercrime with other regional actors and organizations (such as the OAS) and

with multi-stakeholder forums such as the Global Forum on Cyber Experiences (GFCE).

(26) States are encouraged to take the opportunity of negotiating new Convention on combating cybercrime to formulate uniform standards in the field of prevention in order to coordinate the actions of various countries more effectively.

(27) It was recommended to invest in capacity-building to upgrade the skills of officers from the whole spectrum of criminal justice system as an efficient preventive measure against cybercrime of deterrent effect.

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

IV. Organization of the meeting (*continued*)

C. Statements

1. Statements were made by experts from the following Member States: Dominican Republic, Estonia, Guatemala, Malaysia, Peru, South Africa and Viet Nam.