27 July 2020

Original: English

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. In line with the workplan of the Expert Group, the present paragraph contains a compilation of suggestions made by Member States at the meeting under agenda item 3, entitled “Prevention”. These preliminary recommendations and conclusions were made by Member States and their inclusion does not imply their endorsement by the Expert Group, nor are they listed in order of importance:

(1) It should be recognized that prevention is not just the responsibility of governments but requires the participation of all relevant stakeholders, including law enforcement, the private sector, especially Internet service providers, non-governmental organizations, schools and academia, in addition to the public in general.

(2) It was recommended that the public should have easy access to prevention tools such as online platforms, audio clips, plain-language infographics, as well as to reporting platforms.

(3) It was deemed necessary to develop a series of long-term public policies on prevention, which should include the development of awareness-raising campaigns on the safe use of the Internet.

(4) Cybersecurity awareness should be included as a subject in primary, secondary and tertiary education, for both students and teachers. This should ideally be part of a national cybersecurity strategy. States should also share experiences on how to use cybersecurity strategies to prevent cybercrime. In addition, States should devote special attention to preventive measures addressed at youth, including first-time offenders, in order to prevent re-offending.

(5) When preventing and combating cybercrime, States should pay special attention to the issues of preventing and eradicating gender-based violence, violence against women and girls and hate crimes.

(6) Preventive activities must be proactive, regular and continuous and suitable for vulnerable groups.

(7) The intersection of and collaboration between the public and private sectors with big data sets or big data centres can present an area of high vulnerability, in particular but not only in the health sector, in view of the current pandemic. States should devote specific attention to regulating the legal access to such data and protecting it against cybercrime attacks.

(8) Regarding preventive efforts, ISPs should undertake more responsibility for security precautions ("by default") and prevention of cybercrime, and international standards should be developed on the content and duration of log information to be retained by the ISPs. Moreover, ISPs' responsibilities to detect, prevent and disrupt cybercrime should be clearly defined.

(9) Public-private partnerships are needed in preventing and combating cybercrime, including cooperation with cybersecurity stakeholders and big tech companies on information-sharing.

(10) States should provide training to specialized magistrates and judges that handle cybercrime cases and provide investigative bodies with high-performance tools for tracing cryptocurrencies and addressing their use for criminal purposes.

(11) States should step-up strategies to combat the use by traditional criminal groups of cyber tools used to hide their communication and activities.

(12) Solutions should be developed for direct cooperation of national authorities with Internet service providers, while upholding the rule of law and human rights, including data protection requirements.

(13) States should ensure freedom of press when developing measures to prevent cybercrime.

(14) It was recommended to build collective capabilities of competent institutions and to change the prevention culture from reactive to proactive. It was also recommended to put in place a robust mechanism to stimulate and facilitate the sharing of intelligence on potential criminal modus operandi.

(15) Member States are encouraged to continue to include effective prevention measures at the national and international levels and focus on proactive activities such as raising awareness about the risks of cybercrime; targeting the campaigns towards modus operandi such as phishing or malware ("ransomware") and towards different groups such as youth or elderly people; the likelihood of prosecution and punishment of offenders and efforts to prevent crime by identifying and disrupting ongoing illicit activities online. Police department and public prosecution are to invest in detection, signalling and reacting to cybercrime threats. It is important to note that here too, public private partnership is indispensable. These prevention activities do not require extra laws or regulations.

(16) Due to the existence of "digital gap", some developing countries lack the capacity to prevent, detect and combat cybercrime, and are more vulnerable in the face of cybercrime challenges.

(17) UNODC was strongly encouraged to continue providing technical assistance, upon request, to prevent and counter cybercrime.