Distr.: Limited
28 March 2019

English only

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 27–29 March 2019

Draft report

Addendum

III. Summary of deliberations (*continued*)

B. Electronic evidence and criminal justice

1. At its 4th and 5th meetings, on 28 and 29 March respectively, the Expert Group considered agenda item 3, entitled “Electronic evidence and criminal justice”.

2. The discussion was facilitated by the following panellists: Mr. Xioafei Zhai (China); Mr. Markko Kunnapu (Estonia); Ms. Camila Bosch (Chile); Mr. Giuseppe Corasaniti (Italy); Mr. Vadim Smekhnov (Russian Federation); and Ms. Briony Daley Whitworth (Australia).

3. During the subsequent debate, the two-fold role of electronic evidence was noted: on the one hand, it was acknowledged that the use of technology and digital infrastructure created more opportunities for perpetrators of serious and organized crime to expand the scope of their illegal activities, target more victims and increase their profits; on the other hand, it was also stressed that communications data was becoming an increasingly important piece of evidence for the detection, investigation and prosecution of cybercrime and all other crimes.

4. Many speakers referred to the increasing relevance of electronic evidence in criminal proceedings and described varying national approaches to delineating its scope. There is no commonly agreed definition of electronic evidence at the international level. Attention was devoted to the need for procedural legislation granting powers to relevant law enforcement authorities for gathering effectively electronic evidence, in conformity with human rights safeguards. It was noted that investigative powers could range from applying traditional procedural powers, broadly interpreted general investigative powers to a range of cyber-specific measures and dedicated investigative powers implemented to obtain electronic evidence.

5. It was agreed that one of the key steps in cybercrime investigations was to preserve the integrity of electronic evidence and ensure its authenticity and admissibility as evidence in related criminal proceedings. In this context, reference was made to national standards, procedures and requirements needed for handling electronic evidence. The Expert Group again highlighted the necessity of capacity-building and enhanced technical knowledge of competent authorities to deal effectively and efficiently with relevant challenges.

6. The Expert Group considered relevant factors when assessing the admissibility of electronic evidence. Emphasis was placed on the fulfilment of the so-called “proportionality principle” when using special investigative techniques in cybercrime investigations, including the use of undercover agents and remote forensics, especially within the so-called dark web. It was noted that in many domestic legal systems such proportionality was tested primarily by the judicial authority supervising the investigation and by the court, as appropriate. The relevant assessment could be made in light of the seriousness of the offence in question, and or, for instance the number of victims vis-à-vis the intrusion in private life of the specific special investigative techniques used; the types of computer data in question; whether a less restrictive alternative measure was available; whether there has been some measure of procedural fairness in the decision-making process; and whether affected persons have adequate possibilities for legal redress.

7. Attention was drawn to the rise of in-built encryption in software and applications used by persons, thus rendering access to data as electronic evidence difficult and time-consuming without the availability of the proper decryption keys. In response to this challenge, practical suggestions were made, including cooperation with other countries involved that may have the capacity to access encrypted information, the use of the European Cybercrime Centre and the cooperation with the industry which could develop mechanisms for timely access to encrypted data.

8. The use of artificial intelligence in investigations was also mentioned, with particular reference to the examples of facial recognition and copyright violations. In general, artificial intelligence may provide solutions for better use of time and resources when examining large amounts of data in search of important electronic evidence.

IV. Organization of the meeting

B. Statements (*continued*)

9. Statements were made by experts of the following States: Indonesia and Jordan.