Distr.: Limited
27 March 2019

Original: English

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

Draft report

Addendum

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

A. Law enforcement and investigations

1. In line with the workplan, the present paragraph contains a compilation of suggestions made by Member States at the meeting under agenda item 2 entitled "Law enforcement and investigations". These preliminary recommendations and conclusions were submitted by Member States and their inclusion does not imply endorsement by the Expert Group.

III. Summary of deliberations

A. Law enforcement and investigations (*continued*)

2. In the ensuing debate, the Expert Group devoted attention to examples of alleged criminal activities carried out in the digital environment and posing significant difficulties to criminal justice practitioners and investigators when opening or conducting investigations and subsequent prosecutions. Such examples included, inter alia, online fraud, the use of the Internet for terrorist purposes, the use of the dark web to commit illegal activities, as well as the sexual abuse and exploitation of children through the misuse of information and communication technologies. In addition, the Expert Group was informed about the conceptual interdependence of cybercrime and cybersecurity, as well as trends and challenges pertaining to cybercrime, including ransomware attacks; social engineering tactics used for committing fraud (phishing, spear-phishing, vishing, smishing); the use of Cobalt Strike platform for attacks against banking systems; Internet of things; cryptocurrency mining and crypto-jacking; and skimming and associated crimes.

3. The discussion on whether or not a new global comprehensive legal instrument on cybercrime was needed, or, instead, States should focus on effectively implementing existing instruments, including the Council of Europe Convention on Cybercrime (Budapest Convention), was reiterated at the meeting of the Expert Group. On the one hand, it was argued that a new global comprehensive legal instrument on cybercrime was not needed, given that the Budapest Convention

provided an adequate framework for developing appropriate domestic and international cooperation responses to cybercrime. It was recalled that the number of 63 States parties demonstrated that the Budapest Convention was open to accession by non-members of the Council of Europe. Furthermore, it was argued that the convention was used by third State parties to it as a source of inspiration for harmonized domestic legislative standards of both substantive and procedural nature. It was also expressed that the notion of "harmonization of national standards" included not only cases of convergence and common definitions, but also cases where the international norms were "useful" for the development of national regulations. The complementarity of the Budapest Convention with other regional instruments, such as the African Union Convention on Cyber Security and Personal Data Protection (2014) and the International Code of Conduct for Information Security, issued by the Shanghai Cooperation Organisation (SCO), were mentioned.

4. On the other hand, it was noted that a new global legal instrument on cybercrime within the framework of the United Nations was needed to address challenges posed by the fast development of Internet technology that were not covered by existing mechanisms to which not all States in the world were parties to. It was highlighted that such an instrument was envisaged within the framework of a United Nations-led process in which all Member States may develop ownership and responsibility for streamlined efforts towards global responses to cybercrime, taking stock (or building upon) of existing instruments such as the Budapest Convention and the aforementioned African Union Convention. In this context, reference was made to General Assembly resolution 73/187 on "Challenges that Member States face in countering the use of information and communications technologies for criminal purposes" of 18 December 2018 and the mandate contained therein for the Secretary-General to seek the views of Member States on the challenges they face in countering the use of information and communications technologies for criminal purposes and to present a report based on those views, for its consideration at the seventy-fourth session of the General Assembly. In other interventions, the view was expressed that the Budapest Convention did not address the concerns of all United Nations Member States and provides for complex processes to amend its text, which may be a disadvantage in view of the constantly evolving nature of cybercrime.

5. Reference was made to the ongoing negotiation process for the adoption of a second additional protocol to the Budapest Convention aimed at providing clear rules and more effective procedures on the following issues: provisions for more effective and expedited international cooperation; provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests; clearer framework and stronger safeguards for existing practices of transborder access to data; and safeguards, including data protection requirements.

6. It was also stressed that the Organized Crime Convention could be used as a useful tool to address cybercrime challenges particularly in view of their transnational nature. A proposal to consider the negotiation of an additional protocol to the Organized Crime Convention to deal specifically with cybercrime was made.

7. The Expert Group was informed by delegations and panellists about successful national efforts to put in place and implement legal and procedural measures to tackle cybercrime. For some, the Budapest Convention and the accompanying capacity-building projects were essential building blocks in this field. The issue of legislative reforms at the national level was considered thoroughly, including the scope of such reforms. Attention was drawn to the need for inclusive and participatory processes involved to ensure that the voices of different stakeholders were taken on board. Reference was made to the need to ensure legal certainty and clarity based on the principle "nullum crimen nulla poena sine lege" as well as the need for using "technological-neutral" language in new legislation so that it would remain compatible with rapid developments in the field of information and communication technologies.

8. Discussion also revolved around challenges arising from conflicts on enforcement jurisdiction, especially where, for example, a service provider may have its headquarters in one jurisdiction, while the data controller is located in another country or the data is stored in another or in multiple jurisdictions. It was noted that the advent of cloud computing raised additional practical and legal challenges for criminal investigations. It was also noted that flexible approaches to applicable jurisdictional bases in the field of cybercrime might be useful, including, inter alia, by relying more on the place from where ICT services are offered and less on the location where data are residing.

9. The Expert Group also placed emphasis on the need for appropriate procedural powers in place to obtain electronic evidence relating not only to cybercrime, but also to forms of conventional crime. Such electronic evidence may include, among others, subscriber information, content data or traffic data. It was noted that, as new technological developments such as anonymizing software, high-grade encryption and virtual currencies were encountered when investigating offences involving electronic evidence, investigators might need to adopt new strategies and consider how special investigative techniques and remote digital forensics for gathering such electronic evidence could be used while ensuring admissibility and use of such evidence in court.

10. The discussion also focused on how to strike balance between the need for effective law enforcement responses to cybercrime and the protection of fundamental human rights, especially the right to privacy. The common denominator was that, for instance, data retention regulations might represent a pragmatic approach to ensure that communication service providers were able to play a greater role in addressing cybercrime through enhanced cooperation with law enforcement, under the condition that such laws were implemented with due procedural safeguards and privacy protections. Reference was made to the report of the United Nations High Commissioner for Human Rights on “The right to privacy in the digital age”, which was submitted to the Council of Human Rights in accordance with resolution 68/167 of the General Assembly (A/HRC/27/37).

11. The Expert Group reiterated the significance of international cooperation in the cross-border investigation and prosecution of cybercrime. It was acknowledged that the number of requests for mutual legal assistance to obtain or preserve electronic evidence is growing fast, and that current modalities of cooperation, especially lengthy MLA processes, were not sufficient to tackle challenges for speedy and successful access to data due to the volatile nature of such evidence, which could be transferred or deleted “at the click of a mouse”.

12. Different practices were mentioned as examples for fostering international cooperation involving electronic evidence, especially at the operational level, including: the direct transmission of requests for mutual legal assistance among the competent authorities of the cooperating States; the more frequent use of tailor-made international cooperation tools to safeguard the integrity of electronic evidence such as the expedited preservation of computer data; joint investigations (JITs); the use of electronic means to transmit requests for mutual legal assistance, with specific reference to the potential utility of the INTERPOL’s initiative on the secure electronic transmission of mutual legal assistance (e-MLA) exchanges; the sharing of information among contact points of the 24/7 network; and the more frequent use of police-to-police cooperation, including through the assistance of INTERPOL, for purposes of intelligence gathering. Reference was also made to the European Cybercrime Centre (EC3), which was set up by Europol in 2013 to strengthen the EU law enforcement responses to cybercrime.

13. The Expert Group also touched upon the issue of transborder access to data. Overall, it was noted that States’ practices and procedures used, as well as conditions and safeguards to these procedures, varied considerably between different Parties. Further, emphasis was placed on the procedural rights of suspects, privacy

considerations and the protection of personal data, the legality of access to data stored in another jurisdiction, as well as the respect for national sovereignty.

14. The Expert Group stressed the importance of sustainable capacity-building for enhancing the effectiveness and skills of all competent authorities at the operational level to address the challenges posed by cybercrime. In this context, speakers referred to the usefulness of sharing good practices and experiences among practitioners, not only within States but also with other States. Some speakers referred to enhanced training and capacity-building, in conjunction with the development of specialized cybercrime structures or units within prosecution services and law enforcement authorities. It was stressed, in this connection, that, as electronic evidence had become increasingly pervasive in the investigation of conventional crimes as well, the need to put in place specialized structures for the investigation of those crimes with specific expertise, knowledge and operational skills was critical.

15. The Expert Group further discussed, the cooperation of national authorities with the private sector, especially Communication Service Providers (CSPs), to enhance the preservation of, and access to, data. While highlighting the increasing importance of such cooperation at the domestic level, especially in emergency circumstances involving serious crimes, it was also acknowledged that more efforts were needed to ensure a similar level of cooperation in transnational cases. In this regard, the "risk of double compliance" for the CSPs, namely how to balance their responses in view of the legal requirements of the States involved, was mentioned.

IV. Organization of the meeting

B. Statements (*continued*)

16. Statements were made by experts of the following States: Algeria, Burkina Faso, Canada, Chile, China, Colombia, France, India, Italy, Japan, Kuwait, Mauritania, Netherlands, Norway and Sri Lanka.

17. The European Union, an intergovernmental organization, also made a statement.