Distr.: Limited
28 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

A. Law enforcement and investigations (*continued*)

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 their endorsement by the Expert Group, nor does the order of presentation imply an appreciation of their importance:

(a) On the one hand it was suggested that Member States should pursue new international responses against cybercrime by considering the negotiation of a new global legal instrument on cybercrime within the framework of the United Nations which will take into account the concerns and interests of all Member States, taking also into account, among others, the proposed draft United Nations convention on cooperation in combating cybercrime submitted to the Secretary-General on 11 October 2017 (A/C.3/72/12, annex);

(b) On the other hand it was suggested that it was not necessary or appropriate to consider a new global treaty because the challenges of cybercrime and sufficiently trained investigators, prosecutors, and judges are best met with capacity-building, active dialogue and cooperation among law enforcement agencies, and the use of existing tools, such as the Budapest Convention. Following this suggestion Member States should continue using and/or joining existing multilateral legal instruments on cybercrime such as the Budapest Convention, which is considered by many States as the most appropriate and specific guiding tool for developing appropriate domestic legislation – of both substantive and procedural nature – on cybercrime and facilitating international cooperation to combat it;

(c) In view of the transnational nature of cybercrime and the fact that the great majority of global cybercrimes are committed by organized groups, Member States should also make more use of the Organized Crime Convention to facilitate information and evidence sharing for such criminal investigations;

(d) Member States should promote and engage in international cooperation to combat cybercrime, making use of existing instruments as well as by concluding

bilateral agreements using the principle of reciprocity; and by supporting, in collaboration with UNODC, networking and information-sharing among judicial and law enforcement authorities on a regular basis;

(e) Countries should develop police agency expertise in cybercrime investigations by participating in training, which is offered by numerous countries as well as by UNODC and other regional partners and is intended to develop capacities to detect and investigate cybercrime and strengthens collective capacities to fight cybercrime. Capacity-building in this area should particularly address the needs of developing countries, focus on the vulnerabilities of each country in order to ensure tailor-made technical assistance, and promote exchange of state-of-the-art knowledge in the best interest of the beneficiaries;

(f) States are encouraged to continue providing UNODC with the necessary mandates and financial support with a view to delivering tangible results in capacity-building projects in this field;

(g) Countries should devote resources to developing expertise to investigate cybercrime; and to creating partnerships to utilize cooperation mechanisms to obtain critical evidence;

(h) Member States should continue efforts to develop and support specialized cybercrime units, bodies or structures within the law enforcement, the prosecution services and the judiciary, with the necessary expertise and equipment to address challenges posed by cybercrime and for the gathering, sharing and use of electronic evidence for criminal proceedings;

(i) Bearing in mind that cybercrime requires medium- and long-term law enforcement strategies, including cooperation with international partners, to disrupt cybercrime markets, these strategies should be proactive and preferably target organized cybercrime groups, which may have members in numerous countries;

(j) Countries should continue efforts to enact legislation of substantive nature dealing with new and emerging forms of crime in cyberspace in a technologically neutral language to ensure compatibility with future developments in the field of information and communication technologies;

(k) Domestic procedural laws are required to keep pace with technological advancements to ensure law enforcement is adequately equipped to combat online crime. Relevant laws should be drafted with applicable technical concepts in mind as well as the practical needs of cybercrime investigators, consistent with due process guarantees, privacy interests, civil liberties and human rights, as well as the proportionality and subsidiarity principles and safeguards ensuring judicial oversight. Moreover, Member States should devote resources to enacting domestic legislation to authorize:

(i) Requests for expedited preservation of computer data to the person in control of the data – that is, Internet and communications service providers – to keep and maintain the integrity of the data for a specified period of time due to the potential volatility of this data;

(ii) Search and seizure of stored content data from digital devices, which is often the most relevant evidence of an electronic crime to prove attribution;

(iii) Orders to produce computer data that may have less privacy protection, such as traffic data and subscriber data;

(iv) Real-time collection of traffic data and content in appropriate cases; and

(v) Authorization for domestic law enforcement to cooperate internationally.

(l) As cybercrime investigations require creativity, technical acumen, and joint efforts between prosecutor and police, countries should encourage close work between public prosecutors and police early in the investigation to develop sufficient evidence to bring charges against identified subjects;

(m) Law enforcement officers should be guided by investigators when conducting investigations in cybercrime cases to ensure that due process standards are respected;

(n) Domestic law enforcement agencies should reach out to and engage with domestic Internet service providers and other private industry groups. This outreach supports law enforcement investigations by increasing trust and cooperation among stakeholders;

(o) Countries should adopt flexible approaches to applicable jurisdictional bases in the field of cybercrime, including, inter alia, by relying more on the place from where ICT services are offered and less on the location where data is residing;

(p) Countries should invest in educating the community and industry education to enhance their awareness on cybercrime to address the lower rates of reporting cybercrime, compared to other crime types;

(q) Member States should foster public-private partnerships in the field of cybercrime, including through enacting legislation and establishing dialogue channels for this purpose, to promote cooperation between law enforcement authorities and communication service providers as well as academia with a view to enhancing knowledge and on strengthening the effectiveness of responses to cybercrime.

III. Summary of deliberations

A. Law enforcement and investigations (*continued*)

2. Many speakers reported on national measures to develop and implement cybersecurity strategies and policies; enact and/or upgrade legislation on cybercrime; put in place new investigative tools to gather electronic evidence and establish its authenticity for evidentiary purposes in criminal proceedings, taking into account human rights safeguards; implement institutional arrangements geared towards ensuring more efficient use of resources against cybercrime; and promote international cooperation against cybercrime. One speaker referred to the differences between cybersecurity and cybercrime as a main factor for consideration when structuring domestic responses and defining institutional competences on these matters.

3. Many speakers supported the work of the Expert Group as the only comprehensive and most appropriate forum – at the global level – to facilitate discussion and exchange of views among Member States on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen national and international legal or other responses to cybercrime. The added value of the Commission on Crime Prevention and Criminal Justice to the same effect was also mentioned. It was suggested that the Expert Group had a unique mandate to act as a platform for discussions in this field, however this would not necessarily exclude other initiatives aimed at developing comprehensive "global governance" against cybercrime at the international level.

4. Reference was made to a side event organized in the margins of the meeting of the Expert Group on "Approaches in Tackling Cybercrime: Perspectives from across the Pacific and Beyond". The side event was organized by the Government of Australia, the Dominican Republic, Samoa, the United States and Vanuatu.

5. Support was expressed for UNODC's work in the field of technical assistance and capacity-building to build cohesive responses to cybercrime.

6. Moreover, some speakers also expressed appreciation for the release of the Practical Guide for Requesting Electronic Evidence Across Borders. The Guide was jointly drafted and launched by the United Nations Office on Drugs and Crime (UNODC), the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the International Association of Prosecutors (IAP) and was made

available to Member States and their criminal justice officials through UNODC's SHERLOC Portal. Elaborated in collaboration with Member States, other international and regional organizations, and communication service providers such as Facebook, Google, Microsoft and Uber, the Practical Guide contains information to help identify steps at the national level to gather, preserve and share electronic evidence with the overall aim to ensure efficiency in mutual legal assistance practice.

IV. Organization of the meeting

B. Statements (*continued*)

7. Statements were made by experts of the following States: Armenia, Costa Rica, Dominican Republic, Estonia, Georgia, Malaysia, Mexico, Morocco, Paraguay, Peru, Philippines, Slovakia, Spain, Thailand and the United Arab Emirates.

8. The Council of Europe, an intergovernmental organization, also made a statement.