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*)

A. International cooperation

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 2, entitled “International cooperation”. 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) As regards the scope of definition of cybercrime for purposes of international cooperation, countries should ensure sufficient criminalization of cybercrime acts, covering not only cyber-dependent crimes, but also other crimes frequently committed with the use of the Internet and electronic means (cyber-enabled crimes), such as cyber fraud, cyber theft, extortion, money-laundering, trafficking in drugs and arms, child pornography and terrorist activities.

(2) With regard to international cooperation mechanisms, States are encouraged to join and, or use, in the absence of a bilateral MLAT, existing multilateral treaties such as the Budapest Convention and the Organized Crime Convention that provide a legal basis for mutual legal assistance; in the absence of any treaty, States may ask another State for cooperation on the basis of the reciprocity principle; the Budapest Convention should also be used as a standard for capacity-building and technical assistance worldwide, whereas attention is drawn to the ongoing negotiation of the 2nd Additional Protocol to the Budapest Convention to enhance cross-border cooperation further. In another intervention the opinion was reiterated that the Budapest Convention was of limited application because of its nature as regional instrument and its ratification status, as well as lacking of a holistic approach, not taking into account current cybercrime trends and not being fully convenient for developing countries. Attention was drawn to General Assembly resolution 74/247 of 27 December 2019, in which the Assembly decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Still other interventions brought forward that new frameworks or instruments on cybercrime

should not go against existing ones and they should not cause States to abandon or go against current treaties or the commitments previously assumed, as well as agreements that are already in place.

(3) It is necessary to have strategic partners in the investigation of cybercrime, such as the members of existing organizations, including the Organization of American States, G7 or INTERPOL.

(4) In the investigations and judicial proceedings, States' sovereignty and jurisdiction are to be respected. No demands for direct retrieval of data located in another country should be made to any businesses or individuals without prior consent of that country.

(5) The efficiency of international cooperation should be improved by establishing rapid response mechanisms for international cooperation as well as channels of communication through liaison officers and IT systems between national authorities for cross-border collection of evidence and online transfer of electronic evidence.

(6) States should continue strengthening cooperation to protect critical infrastructure and strengthen networks of collaboration among computer emergency response teams (CERTs and CSIRTs).

(7) States should consider the creation of innovative protocols for the exchange of information, including intelligence and evidences of criminal acts, in order to expedite such procedures.

(8) There is the need for a renewed confirmation of the commitment of all Member States to ensuring the safety and security of the ICTs through solely peaceful use and strengthening the international efforts to combat any malicious activities on cyberspace in times of major crisis on global, regional and local levels.

(9) The procedures for international cooperation should be optimized so that maximum assistance is provided within the possibilities derived from a domestic legal framework for international cooperation requests concerning preservation of electronic evidence, access to log information and user registration information which does not interfere with human rights and fundamental freedoms or property rights.

(10) Countries are called upon to pay particular attention to the necessary proportionality of the investigative measures, while respecting fundamental freedoms and the personal data protection regimes associated with private correspondence.

(11) International cooperation to combat cybercrime should also take into account gender- and age-sensitive approaches and the needs of vulnerable groups.

(12) In terms of the scope of international cooperation, while mutual legal assistance should be provided only by national authorities, cooperation should not be limited to government departments but should also involve the private sector such as Internet Service Providers (ISPs). In this context, it was recommended that provisions needed to be adopted allowing for the direct cooperation with ISPs in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests.

(13) Options to counter cybercrime and to protect societies must always ensure the protection of human rights and constitutional guarantees and promote a more free, open, secure and resilient cyberspace for all.

(14) Countries are encouraged to streamline cooperation with the industry, and enhance collaboration between government and private service providers, particularly for addressing the challenges posed by the harmful criminal material on the Internet.

(15) Private companies, notably ISPs, have shared responsibility in preventing and investigating cybercrime; such companies should expedite and expand their responses to legal assistance requests, offer them in the countries where they are

based, and ensure they have appropriate channels for communicating with local authorities.

(16) Public-private partnerships must be strengthened; where such partnerships do not exist, they must be created, private companies should participate in working groups (multilateral forums) and be a part of the conversation on enhancing the approach towards cybercrimes.

(17) Non-governmental organizations and academia must also form part of efforts to prevent and counter cybercrime, as they provide an inclusive, plural and comprehensive perspective, inter alia to ensure the protection of human rights, especially freedom of expression and privacy.

(18) Countries are called upon to join, make wider use of and strengthen authorized networks of practitioners to preserve and exchange admissible electronic evidence, including 24/7 networks, specialized networks on cybercrime and INTERPOL channels for prompt police-to-police cooperation, as well as networking with strategically aligned partners, with a view to sharing data on cybercrime matters and enabling rapid responses and minimize loss of critical evidence. Interventions also recommended the use of police-to-police cooperation and other methods of informal cooperation before using MLA channels.

(19) Each State to set up a genuine 24/7 point of contact, accompanied by appropriate resources, to facilitate the preservation of digital data alongside traditional international mutual assistance in criminal matters, drawing on the successful model of data freezing under the Council of Europe Convention.

(20) Countries should strengthen inter-institutional collaboration, and improve interoperability through standardization of information requests and authentication procedures and multi-stakeholder buy-in.

(21) Countries should improve the implementation of national laws and enhance improved domestic coordination and synergy for the collection and sharing of information and evidence for prosecution purposes.

(22) States should strengthen measures for sharing financial or monetary information, freezing of accounts and confiscation of assets to ensure that criminals cannot enjoy the benefits of criminal activities.

(23) States are encouraged to establish joint investigative teams with other countries at the bilateral, regional or international levels to enhance enforcement capabilities.

(24) States should also enable the effective handling of electronic evidence and its admissibility before the court, including where it is destined for, or received from, a foreign jurisdiction. In this regard, countries are encouraged to continue or start reform efforts with regard to legislation on cybercrime and electronic evidence, following positive examples and reforms worldwide.

(25) It is recommended to develop legal frameworks which also include aspects of extraterritorial jurisdiction over cybercrime acts.

(26) Countries should refine mechanisms to mitigate conflicts, and address the challenges of attribution and capacity to investigate cybercrime cases.

(27) States should work towards standardizing and disseminating procedural tools for expedited production of data and extending searches (such as production orders, as well as orders for expedited preservation or trans-border access, etc.) to facilitate the work of law enforcement authorities and their direct cooperation with ISPs and solve problems associated with the tracing of electronic evidence and its appropriate use.

(28) States should facilitate the development and standardization of interoperable technical standards for digital forensics and cross-border electronic evidence retrieval.

(29) It is recommended to invest in a strong central authority for international cooperation in criminal matters to ensure effectiveness of cooperation mechanisms involving cybercrime as well; it is recommended to establish specific units to investigate cybercrime; and also to address preservation requests by another State through a 24-7 network (or directly with the provider in some circumstances) to preserve needed data as quickly as possible. Increased understanding of the information needed for a successful MLA request may assist in obtaining the data more quickly.

(30) Effective international cooperation requires national laws which create procedures that enable international cooperation. Thus, national laws must permit international cooperation among law enforcement agencies.

(31) Beyond domestic laws, international cooperation on cybercrime relies on both formal, treaty-based cooperation and traditional police-to-police assistance. When we debate a new instrument on cybercrime, it is important that countries remember that a new instrument should not conflict with existing instruments, which already enable real-time international cooperation for so many. Thus, countries should ensure that any new instrument on cybercrime avoids conflict with existing treaties.

(32) Sustainable capacity-building and technical assistance to increase capabilities across operational areas and strengthen the capacity of national authorities to respond to cybercrime should be prioritized and increased, including networking, joint meetings and trainings, sharing best practices, training materials, and templates for cooperation. Such capacity-building and training should include highly specialized training for practitioners that promotes, in particular, the participation of female experts, and further address the needs of legislators and policymakers to better handle issues of data retention for law enforcement purposes; law enforcement authorities, investigators and analysts to improve their ability in forensics and use of open source data for investigations and on the chain of custody for electronic evidence; and in collecting and sharing electronic evidence abroad; and judges, prosecutors, central authorities and lawyers to effectively adjudicate and deal with relevant cases.

(33) It is imperative to develop adequate, and if possible uniform, data retention/data preservation rules and timelines to ensure that electronic evidence can be preserved or obtained to support further MLA requests.

(34) The Group of 77 and China recognizes that international cooperation is important for gathering and sharing electronic evidence in the context of cross-border investigations and the need for fast and effective responses to requests for mutual legal assistance related to preserving and obtaining electronic evidence. The Group also emphasizes that the principles of sovereignty and reciprocity should be respected in the process.

(35) The Group of 77 and China likewise encourages UNODC to further provide capacity-building and training programmes in combating cybercrime to national governmental experts, to strengthen capacities to detect and investigate cybercrime. Such capacity-building should address the needs of developing countries, focus on the vulnerabilities of each country in order to provide tailor-made technical assistance and promote the exchange of the most up-to-date knowledge in the best interests of the practitioners and stakeholders.

(36) UNODC has developed the “Mutual Legal Assistance Request Writer Tool” to assist criminal justice practitioners in drafting MLA requests. UNODC has also developed the “Practical Guide for Requesting Electronic Evidence Across Borders”, available on request to government practitioners in Member States. Thus, countries may benefit from employing these key tools developed by UNODC.

(37) The CCPCJ should consider extending the workplan of the IEG beyond 2021 as a forum for practitioners to exchange information on cybercrime.

(38) It was recommended by some speakers that the negotiation and adoption of a United Nations Convention to promote cooperation in combating cybercrime would facilitate improving the efficiency of international cooperation in the fight against cybercrime.

(39) It was recommended that any elaboration of a new Convention should be handled among the experts in UNODC in Vienna.

IV. Organization of the meeting (*continued*)

C. Statements

2. Statements were made by experts from the following Member States and non-member observer State: Algeria, Argentina, Armenia, Brazil, Canada, Chile, Colombia, Ecuador, Egypt, India, Lebanon, Mexico, Netherlands, Norway, Portugal, Romania, Russian Federation, State of Palestine, State of Palestine on behalf of the Group of 77 and China, United States of America.