Distr.: Limited
29 March 2019

English only

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*)

B. Electronic evidence and criminal justice

1. Discussion was devoted to subscriber information as the type of data most often sought by criminal justice authorities in criminal investigations of cybercrime and other cases involving electronic evidence. In this connection, many speakers referred to challenges relating to subscriber information related to a specific IP address used in a criminal offence. It was noted that, while "static" IP addresses are stable and assigned to a specific subscriber for the duration of the service arrangement and while a service provider can look up such information in a database of subscribers, a service provider may assign an IP address to multiple users. Thus, the need is raised to determine the subscriber to whom the IP address has been assigned at a specific moment in time. It was also noted that the reason for the dynamic allocation of IP addresses is that, under Internet Protocol version 4 (IPv4), the available numbers are limited; and that the problem will eventually be resolved once the transition to IP version 6 has been completed or is more advanced.

2. The Expert Group also discussed the issue of differentiation of types of requested data and its impact on the effectiveness and timeliness of international cooperation mechanisms to obtain electronic evidence. Solutions examined were related, among others, to strengthening law enforcement cooperation and continuing the multilateral dialogue on transnational access to computer data; and establishing a separate regime for access to subscriber information, as defined in article 18, paragraph 3 of the Council of Europe Convention on Cybercrime.

3. Many speakers referred to the challenges posed by cryptocurrencies in cybercrime investigations. The Expert Group was informed about the UNODC Cryptocurrency Investigation Train-the-Trainers course. The aim of the training is to upgrade the capacity of law enforcement officers, analysts, prosecutors and judges in relation to cryptocurrencies, tracing bitcoins in a financial investigation, locating information resources and collaborating on international casework.

4. The Expert Group continued, under this agenda item, to discuss jurisdictional issues with particular reference to recent developments in national jurisprudence

regarding the interpretation of the territoriality principle in cases where computer data were stored in cloud servers in other jurisdictions.

5. Speakers agreed that international cooperation was of paramount importance for gathering and sharing electronic evidence in the context of cross-border investigations. It was stressed that States should make full use of the Organized Crime Convention, relevant regional and bilateral treaties and arrangements on cybercrime to foster international cooperation on judicial assistance and law enforcement in related cases, while the sovereignty of each other and equality and reciprocity. The significance of promoting networking for sharing of experiences and expertise was highlighted, particularly in order to address the challenges posed by varying national requirements on the admissibility and evidentiary integrity and authenticity of such evidence.

6. Priority was accorded by many speakers to the need for sustainable capacity building at the levels of national law enforcement and criminal justice systems, including practitioners from central authorities involved in international cooperation. It was noted that such capacity building was essential particularly for developing countries, both in terms of human resources and infrastructure and equipment, and with a view to bridge the digital divide with developed countries. Overall, it was agreed that building the capacity of law enforcement and criminal justice actors to combat cybercrime would be an ongoing and continuous process, as technology and criminal innovations continue at a rapid pace. Thus, the vast majority of speakers referred to technical assistance and cooperation as important prerequisites to enhance domestic capabilities, but also to enable the sharing of good investigative practices, experience and the dissemination of new techniques.

7. In this connection, a number of speakers referred to the challenges of limited resources in the field of forensics, lack of forensic tools and equipment, which are often expensive, and difficulties that arise from the sheer quantity of collected data for analysis. Challenges in recruiting personnel with sufficient skills were also reported.

8. Reference was made to the “No More Ransom” project, a public-private initiative launched in 2016 by the Dutch national police, Europol, McAfee and Kaspersky Lab, with the aim to reduce the risk of proliferation of malware products and minimize the damage of victims.

III. Summary of deliberations (*continued*)

B. Electronic evidence and criminal justice

9. In line with the workplan, the present paragraph contains a compilation of suggestions made by Member States at the meeting under agenda item 3 entitled “Electronic evidence and criminal justice”. These preliminary recommendations and conclusions were submitted by Member States and their inclusion does not imply endorsement by the Expert Group, nor does the order of presentation imply an appreciation of their importance.

(a) Member States should develop and implement legal powers, jurisdictional rules and other procedural provisions to ensure that cybercrime and crimes facilitated by the use of technology can be effectively investigated at the national level and that effective cooperation can be obtained in transnational cases, taking into account the need for effective law enforcement, national sovereignty and the need to maintain effective protections for privacy and other human rights. This may include:

(i) The adjustment of rules of evidence to ensure that electronic evidence can be collected, preserved, authenticated and used in criminal proceedings;

(ii) The adoption of provisions dealing with the national and international tracing of communications;

(iii) The adoption of provisions governing the conduct of domestic and cross-border searches;

(iv) The adoption of provisions dealing with the interception of communications transmitted via computer networks and similar media;

(v) To enact both substantial and procedural laws that are technologically neutral to enable countries to tackle new and emerging forms of cybercrime;

(vi) Harmonization of national legislation; and

(vii) Enacting or improving legislation to recognize the admissibility of electronic evidence and provide for the definition and scope of electronic evidence.

(b) Member States should foster capacity building of law enforcement personnel, including specialized law enforcement structures, prosecutors and the judiciary to be able to have at least basic technical knowledge on electronic evidence and to respond effectively and expeditiously to requests for assistance in the tracing of communications and other measures necessary for the investigation of cybercrime;

(c) Member States should foster capacity building to improve investigations, get better understanding of cybercrime and the equipment and technologies to fight cybercrime, as well as for prosecutors, judges and central national authorities to appropriately prosecute and adjudicate on cybercrime;

(d) Capacity building of central authorities involved in international cooperation on MLA requirements and procedures, including training on the drafting of sufficient requests for electronic evidence, should be pursued;

(e) Member States should consider the “prosecution team” approach, which combines the skills and resources of various agencies to bring together prosecutors, investigative agents, and forensic analysts to pursue an investigation, and which would allow prosecutors to handle and present electronic evidence;

(f) The admissibility of electronic evidence should not depend on whether evidence was collected from outside a country’s jurisdiction, as long as the reliability of the evidence is not impaired and the evidence is lawfully collected, for example, pursuant to an MLA agreement, multilateral agreement, or in cooperation with the country that has jurisdiction;

(g) Member States should take necessary measures to enact legislation to ensure the admissibility of electronic evidence bearing in mind that admissibility of evidence, including electronic evidence, is an issue that each country should address according to its domestic law;

(h) Member States should enhance international cooperation among law enforcement agencies, prosecutors and judicial authorities as well as with ISPs to bridge the gap between the speed at which cybercriminals operate and the pace of law enforcement responses. In doing so, Member States should utilize existing frameworks, such as the 24/7 networks and cooperation through Interpol as well as MLAs to foster international cooperation involving electronic evidence. Member States should further harmonize and streamline MLA processes and develop a common template to expedite MLA processes for collection and transfer of cross-border electronic evidence in a timely manner;

(i) Member States are encouraged to enhance experience and information-sharing, including national legislation, national procedures, best practices on cross-border cybercrime investigations, information on organized criminal groups and the techniques and methodology used by organized cyber-criminal groups;

(j) Member States should develop network of focal points between law enforcement agencies, judicial authorities and prosecutors;

(k) Member States should evaluate the possibility having the Expert Group or UNODC experts conduct an annual assessment of cybercrime trends and newly

developed cybercrime threats with the contribution from Member States, to be publicly available;

(l) UNODC should support the expansion of research activities to identify new forms of offending, new patterns of offending, the effects of offending in key areas, as well as rapidly evolving telecommunications environment, including the expansion of the Internet of things, the adoption of block-chain technologies and crypto-currencies, and the use of artificial intelligence in conjunction with machine learning;

(m) Through the United Nations Global Programme on Cybercrime, UNODC should promote, support and implement, as appropriate, technical cooperation and assistance projects, subject to the availability of resources. Such projects would bring together experts in crime prevention, computer security, legislation, prosecution, investigative techniques and related matters with States seeking information or assistance in those areas;

(n) UNODC should establish an educational programme focused on raising the level of knowledge and awareness of cybercrime counteraction, especially in the sphere of electronic evidence gathering, for the judicial and prosecution authorities of Member States;

(o) Member States should pursue action to enhance cooperation in gathering electronic evidence, including the following:

(i) Sharing of information on cybercrime threats;

(ii) Sharing of information on the organized cybercriminal groups, including the techniques and methodology used by organized cybercriminal groups;

(iii) Fostering enhanced cooperation and coordination among law enforcement agencies, prosecutors and judicial authorities;

(iv) Sharing national strategies and initiatives in tackling cybercrime, including national legislation and procedures to bring cybercriminals to justice;

(v) Sharing of best practices and experiences related to cross-border cybercrime investigation;

(vi) Developing a network of point of contacts between LEAs, judicial authorities and prosecutors;

(vii) Harmonizing and streamlining MLA process and developing a common template to expedite MLA process for collection and transfer of cross-border electronic evidence in timely manner;

(viii) Holding workshops/seminars to strengthen capability of LEAs and judicial authorities for drafting MLAT request for collection of evidence in cybercrime related matters;

(ix) Evolving standards and uniformity in procedural aspects of collection and transfer of digital evidence;

(x) Developing a common approach on information sharing arrangement with service providers for cybercrime investigations and evidence gathering;

(xi) Engaging with service providers, through public-private partnership, to work out modalities of cooperation in law enforcement, cybercrime investigation and evidence collection;

(xii) Developing Guidelines for service providers to assist law enforcement agencies in cybercrime investigation, including format and duration for preservation of digital evidence and information;

(xiii) Strengthening the techno-legal capacity of Law enforcement agencies, judges, prosecutors through capacity building and skill development programmes;

(xiv) Assistance to developing countries in strengthening cyber forensic capabilities, including setting up of cyber forensic laboratories;

(xv) Holding workshops/seminars to disseminate awareness about best practices to address the cybercrime; and

(xvi) Establishing an international agency to validate and certify digital forensics tools, preparing manuals and capacity building for law enforcement and judicial response to cybercrime.

(p) Countries should invest in the need for building and enhancing digital forensics capabilities, including training and security certifications, as well as Information Security Management Systems (ISMS);

(q) States should take measures to encourage the Internet Service Providers (the ISPs) to play a role on preventing cybercrime and supporting law enforcement and investigation, including establishing in their domestic legislation the obligation of the ISPs in this regard, and clearly define the scope and boundary of such obligation in order to protect the legitimate rights and interests of the ISPs;

(r) States should strengthen investigation and law enforcement against acts of aiding, abetting and preparation of cybercrime, with a view to effectively addressing the complete chain of cybercrime;

(s) States should continue to strengthen capacity building and enhance the necessary capability of the judicial and law enforcement authority in investigating and prosecuting cybercrime. The increasing challenges posed by cloud computing, dark web and other emerging technologies should be emphasized in capacity building. Moreover, States are encouraged to provide capacity building assistance to developing countries;

(t) States should improve the effectiveness of domestic inter-agency coordination and synergies, including sharing of trusted information and intelligence, with the private sector, civil societies and other stakeholders as an enabler of efficient international cooperation and collaboration.

IV. Organization of the meeting

B. Statements (*continued*)

10. Statements were made by experts of the following States: Germany and Viet Nam.