Distr.: Limited
4 April 2018

English only

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 3–5 April 2018

Draft report

Addendum

II. Recommendations

Legislation and frameworks (agenda item 2)

1. In line with the Chair's proposal for the 2018–2021 workplan of the Expert Group, adopted by the meeting on its 1st day, at the meetings of the Expert Group in 2018, 2019 and 2020, the Rapporteur, with the necessary assistance of the Secretariat and based on the discussions and deliberations, will prepare a list of preliminary conclusions and recommendations suggested by Member States, which should be precise and focus on strengthening practical responses to cybercrime. Following the workplan, the list is included in the summary report of the meeting as a compilation of suggestions made by Member States, for further discussion at the stock-taking meeting in 2021. As worded in the workplan the Expert Group at the stock-taking meeting will consider the accumulated preliminary conclusions and recommendations in order to produce a consolidated and comprehensive list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.

2. Accordingly, the following is the compilation of suggestions made by Member States at the fourth session of the Expert Group in relation to agenda item 2 "Legislation and frameworks":

(a) Member States should, in order for legislative provisions to withstand the test of time with regard to future developments in technology, enact technologically neutral formulated laws that criminalize the activity deemed illegal instead of the means used. Member States should also consider establishing consistent terminology to properly describe the different types of cybercrime activities and facilitate, to the extent possible, accurate interpretation of relevant laws by law enforcement agencies and the judiciary;

(b) Member States should respect the sovereign rights of other States in formulating policies and legislation that meet their national conditions and needs in addressing cybercrime. To foster international cooperation to combat cybercrime, the principle of sovereignty should not be mistakenly interpreted as an obstacle and rather be respected as a fundamental starting point. Volatility of electronic transport and storage of data, such as in so-called clouds, may call for engaging in multilateral

discussions on innovative and expanded mutual assistance between States to ensure timely access to electronic data and evidence;

(c) In order to deny the existence of "safe havens" Member States should offer each other cooperation to the widest extent possible in investigation, evidence collection, prosecution, adjudication and if necessary the removal of illegal content on the Internet. Member States should also provide for the greatest degree of flexibility when providing international cooperation in relation to cybercrimes and other crimes involving electronic data, either as leads in investigations, and, or, as evidence, irrespective of whether the underlying activity is denominated differently in the respective States. In doing so, Member States should bear in mind that dual criminality is usually required for extradition though not necessarily for mutual legal assistance;

(d) Member States should consider, in formulating policies and legislation, the need for striking a balance between human rights protection on the one hand, and national security, public order and legitimate rights of third persons, on the other. National legislations that criminalize conduct and provide for procedural legal authority to permit investigation, prosecution and adjudication of cybercrimes should be consistent with due process guarantees, privacy interests, civil liberties and human rights. National policies and legislations, as well as internationally used and or to be developed instruments should be multidimensional in their approach, on the one hand sharing adequate cybercrime policies from an encompassing understanding of the broader concept of cybersecurity, and on the other hand cover not only illegal behaviour but also focus on prevention of crimes, offering help to individual victims of crime and, or, offer perspectives for the general public to remove from the consequences of cybercrimes. In order to create a solid base for international cooperation on combating cybercrime Member States should strive to find and promote a culture of establishing a common future for cyberspace;

(e) Member States should pursue international cooperation without requiring full harmonization of national legislation as long as the underlying conduct is criminalized, and laws are sufficiently compatible to simplify and expedite the various forms of such cooperation;

(f) Member States should develop, if they have not done so, legislation to provide for extraterritorial jurisdiction over their nationals or ordinary residents to offences irrespective of where the offence occurred and whether the same is regarded as an offence in the foreign jurisdiction;

(g) Member States may draw on different legal bases for international cooperation including reciprocity, as well as bilateral or multilateral treaties and other arrangements. Moreover, Member States with more advanced capacities in the field of cybercrime should assume more responsibilities — proportionate to their capacities or infrastructure — in providing legal assistance to other States;

(h) Member States should consult all relevant stakeholders, including intergovernmental stakeholders, the private sector and civil society, as early as possible when the decision is made to bring forward cybercrime legislation to ensure that relevant issues are properly considered;

(i) Member States should foster strong and trustworthy public-private cooperation in the field of combating cybercrime, including cooperation between government law enforcement authorities and communication service providers (CSPs). Engaging in dialogue with private industry, if possible accompanied by public private partnerships and if needed MOU's is also required to strengthen and facilitate cooperation;

(j) Member States should support UNODC in establishing an educational project/programme focusing on awareness-raising among judicial and prosecution authorities and digital forensic experts of Member States, as well as private entities, about cybercrime and appropriate responses to it; and use capacity-building tools, or

an electronic knowledge management platform to similarly raise awareness of civil society about the impact of cybercrime;

(k) Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by capacity-building measures and technical assistance programmes. Member States should allocate appropriate resources for domestic capacity-building. The proper implementation of cybercrime-related legislation requires the training of police and prosecutors, as well as public awareness campaigns. Such resources will also further international cooperation as such cooperation is enhanced by country's domestic capacity to investigate and prosecute cybercrime-related offences;

(l) UNODC should engage actively in capacity-building for all Member States in need of assistance, especially developing countries. Such capacity-building activities should be politically neutral and free of condition, result from thorough consultations and be voluntarily accepted by recipient countries. In terms of substance, those capacity-building activities should cover at least the following areas:

(i) Training for judges, prosecutors, investigators and law enforcement authorities in cybercrime investigations, handling of electronic evidence, chain of custody and forensic analysis;

(ii) Drafting and/or amendment as well as implementation of legislation on cybercrime and electronic evidence;

(iii) Structuring cybercrime investigation units and providing guidance on related procedures;

(m) UNODC should seek synergies and cooperate closely with other stakeholders or organizations such as the Council of Europe and the Organization of American States in the field of capacity-building programmes on legislation to ensure that activities and initiatives in this area are not dispersed or fragmented;

(n) Member States should continue using the Expert Group as a platform for exchange of information and best practices, including model laws or model clauses, on such issues as jurisdiction, special investigative techniques, as well as electronic evidence, including challenges posed by its volatile nature and admissibility in court, and international cooperation;

(o) Member States should explore relevant universally accepted practices and rules through multilateral consultation under the auspices of the United Nations and through the Expert Group platform, to avoid fragmentation;

(p) Member States should evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on a regular basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(q) Member States should develop a new international legal instrument on cybercrime within the framework of the United Nations which would take into account the concerns and interests of all Member States;

(r) Member States should use, and, or join existing multilateral legal instruments on cybercrime such as the Budapest Convention as they are evaluated by many States as a best practice model guiding appropriate domestic and international responses to cybercrime;

(s) Existing legal instruments and mechanisms, in particular the United Nations Convention against Transnational Organized Crime should be taken advantage of by as many States as possible to strengthen international cooperation;

(t) Under the auspices of the expert group member States should explore, drawing on best practices in existing regional instruments and/or national legislation, internationally applicable responses, which could be elaborated in the form of model laws or model clauses, where appropriate.