Seventh session of the of the Open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, 6-8 April 2021

Agreed paragraphs

(Status: 7 April, 2 PM)

Legislation and frameworks

(a) Member States should ensure that their legislative provisions withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used. Member States, where they deem necessary and appropriate, should also consider establishing consistent terminology to describe cybercrime activities at the domestic level and facilitate, to the extent possible, accurate interpretations of relevant laws by law enforcement agencies and the judiciary;

(k) Member States should support UNODC in establishing an educational project or programme that focuses on raising awareness of cybercrime and appropriate responses to it among judicial and prosecution authorities, digital forensic experts of Member States and among private entities, and use capacity-building tools or an electronic knowledge management platform to raise awareness of the impact of cybercrime among civil society;

(n) UNODC should engage actively in capacity-building for all Member States in need of assistance, in particular developing countries. Such capacity-building activities should be politically neutral and free from conditions, should result from thorough consultations and be voluntarily accepted by the 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, the handling of electronic evidence, chain of custody and forensic analysis;

Criminalization

(a) Member States should take into account that many substantive criminal law provisions designed for "offline" crime may also be applicable to crimes committed online. Therefore, to strengthen law enforcement, Member States should use existing provisions in domestic and international law, as appropriate, to tackle crimes in the online environment;

(f) To the extent that they have not done so already, Member States should consider the criminalization of:

> (vii) Illegally gaining access to or hacking into computer systems;
>
> (viii) Illegally intercepting or damaging computer data and damaging computer systems;
>
> (ix) Illegally interfering with computer data and systems;

(l) Member States should explore ways to help to ensure that the exchange of information among investigators and prosecutors handling cybercrime is made in a timely and secure way, including by strengthening networks of national institutions that may be available 24/7;

Law enforcement and investigation

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

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

(k) Domestic procedural laws must keep pace with technological advances and ensure that law enforcement authorities are adequately equipped to combat cybercrime. Relevant laws should be drafted taking into account applicable technical concepts and the practical needs of cybercrime investigators, consistent with due process, privacy, human rights and fundamental freedoms. Moreover, Member States should devote resources to enacting domestic legislation that authorizes:

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

(v) International cooperation by domestic law enforcement authorities;

(p) Countries should invest in raising awareness of cybercrime among the general public and private industry in order to address the lower rates of reporting of cybercrime compared with other types of crime;

Electronic evidence and criminal justice

(a) Member States should develop and implement legal frameworks, jurisdictional rules and other procedural provisions to ensure that cybercrime can be effectively investigated at the national level and that effective international cooperation can be achieved in that regard through effective law enforcement, with respect for national sovereignty, and the protection of privacy and all 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 on the national and international tracing of communications;

(b) Member States should foster efforts to build the capacity of law enforcement personnel, including those working in specialized law enforcement structures, prosecutors and the judiciary, so that such personnel possess at least basic technical knowledge of electronic evidence and are able to respond effectively and expeditiously to requests for assistance in the tracing of communications and undertake other measures necessary for the investigation of cybercrime;

(g) Member States should take necessary measures to enact legislation that ensures 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;

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

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

(o) Member States should make efforts to enhance cooperation in gathering electronic evidence. In this regard they are encouraged to consider, inter alia, the following:

(i) Sharing of information on cybercrime threats;

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

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

(xi) Engagement with service providers through public-private partnerships in order to establish modalities of cooperation in law enforcement, cybercrime investigations and evidence collection;

(xii) Development of guidelines for service providers to assist law enforcement agencies in cybercrime investigations, including with regard to the format and duration of preservation of digital evidence and information;

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

(xv) Holding of workshops and seminars to raise awareness of best practices in addressing cybercrime;

(q) In legal systems that use the inquisitorial model, where judicial officers are also investigators, the judiciary should receive specialized training on cybercrime;

(u) States may consider establishing the following data as electronic evidence in their domestic legislation: traffic data, such as log files; content data, such as emails; subscriber data, such as user registration information; and other data that are stored, processed and transmitted in a digital format and that are produced during the commission of a crime and can therefore be used to prove the facts of that crime;

International cooperation

(e) 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 information technology systems between national authorities for the cross-border collection of evidence and online transfer of electronic evidence;

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

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

(p) Countries are encouraged to streamline cooperation with industry and enhance collaboration between the Government and private service providers, in particular for addressing the challenges posed by harmful criminal material on the Internet;

(t) 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 minimizing loss of critical evidence. The use of police-to-police cooperation and other methods of informal cooperation before using mutual legal assistance channels was also recommended;

(v) Member States should exchange information on how challenges in accessing digital evidence in a timely manner are being resolved domestically, in order for other Member States to benefit from those experiences and increase the efficiency and effectiveness of their own processes;

(w) Member States should establish practices that allow the transmittal and receipt of mutual legal assistance requests through electronic means to reduce delays in the State-to-State transmission of documents;

(y) Countries should improve the implementation of national laws and enhance improved domestic coordination and synergies for the collection and sharing of information and evidence for prosecution purposes;

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

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

(mm) 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 through networking, joint meetings and training, the sharing of 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 should address the needs of legislators and policymakers to better handle issues of data retention for law enforcement purposes. The capacity-building and training should also be focused on improving the abilities of law enforcement authorities, investigators and analysts in forensics, in the use of open source data for investigations and in the chain of custody for electronic evidence, as well as in collecting and sharing electronic evidence abroad. Another focus of the capacity-building and training should be on improving the abilities of judges, prosecutors, central authorities and lawyers to effectively adjudicate and deal with relevant cases;

(oo) International cooperation is important for gathering and sharing electronic evidence in the context of cross-border investigations and for fast and effective responses to requests for mutual legal assistance related to preserving and obtaining electronic evidence. The principles of sovereignty and reciprocity should be respected in the process;

(pp) UNODC is encouraged 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 practitioners and stakeholders;

(qq) UNODC has developed the Mutual Legal Assistance Request Writer Tool to assist criminal justice practitioners in drafting mutual legal assistance requests. The Office has also developed the Practical Guide for Requesting Electronic Evidence Across Borders, available on request to government practitioners in Member States. Countries may benefit from employing those key tools developed by UNODC;

(yy) There were calls for the active participation of all Member States in the work of the ad hoc committee to develop a new convention;

(ccc) Member States should consider investing in specialized centralized cybercrime forces and in regional technological units for criminal investigations;

(ddd) Member States should also consider establishing separate cybercrime units within central authorities for mutual legal assistance as a base of expertise in the complex area of international cooperation. Such specialized units not only provide benefit in the day-to-day practice of mutual legal assistance, but also allow for focused capacity-building assistance such as training to address the needs of domestic and foreign authorities on how to obtain mutual legal assistance involving electronic evidence quickly and efficiently in cyber-related matters;

(eee) Member States should consider maintaining electronic databases that facilitate access to statistics relating to incoming and outgoing requests for mutual legal assistance involving electronic evidence, to ensure that reviews of efficiency and effectiveness are in place;

(fff) Member States should be reminded to utilize central authorities in transmitting requests for mutual legal assistance and in working with competent authorities for the execution of such requests to ensure compliance with existing treaties and to reduce delays in the process;

Prevention

(a) It should be recognized that prevention is not just the responsibility of Governments: it also requires the participation of all relevant stakeholders, including law enforcement authorities, the private sector, especially Internet service providers, non-governmental organizations, schools and academia, in addition to the public in general;

(b) It was recommended that the public should have easy access to prevention tools such as online platforms, audio clips, plain-language infographics and reporting platforms;

(c) It was deemed necessary to develop a series of long-term public policies on prevention, which should include the development of awareness-raising campaigns on the safe use of the Internet;

(e) When preventing and combating cybercrime, States should pay special attention to the issues of preventing and eradicating gender-based violence, in particular, violence against women and girls, and hate crimes;

(f) Preventive activities must be proactive, regular, continuous and suitable for vulnerable groups;

(j) States should provide training for specialized magistrates and judges who handle cybercrime cases and provide investigative bodies with high-performance tools for tracing cryptocurrencies and addressing their use for criminal purposes;

(n) It was recommended that the collective capabilities of competent institutions be built and the prevention culture changed from reactive to proactive. It was also recommended that a robust mechanism to stimulate and facilitate the sharing of intelligence on potential criminal modi operandi be put in place;

(o) Member States are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities such as raising awareness about the risks of cybercrime, targeting such campaigns at modi operandi such as phishing or malware (“ransomware”) and at different groups such as youth and elderly people. Member States are also encouraged to continue to focus on the likelihood of prosecution and punishment of offenders and efforts to prevent crime by identifying and disrupting ongoing illicit activities online. Police and public prosecution services should invest in signalling, detecting and reacting

to cybercrime threats. Public-private partnership is indispensable. These prevention activities do not require extra laws or regulations;

(p) Owing to the existence of the "digital gap", some developing countries lack the capacity to prevent, detect and combat cybercrime and are more vulnerable in the face of cybercrime challenges;

(q) UNODC was strongly encouraged to continue providing technical assistance, upon request, to prevent and counter cybercrime;

(v) Member States are encouraged to continue to include effective prevention measures at the national and international levels and to focus on proactive activities, such as raising awareness about the risks of cybercrime and the likelihood of prosecution and punishment for offenders and efforts to prevent further crime, by identifying and disrupting ongoing illicit online activities;

(x) Countries should collect a broad range of data to help understand trends to inform and shape cybercrime policies and operational responses to combat cybercrime;

(y) Efforts in the development of strategies for cybercrime prevention should also take into account the protection of human rights;

(z) "Criminal justice capacity" should be another area of focus in national cybercrime strategies. Assistance to developing countries should be a priority in order to strengthen law enforcement capacity in preventing cybercrime;

(bb) States should develop or strengthen support programmes for victims of cybercrime;

(cc) States should undertake surveys to measure the impact of cybercrime on businesses, including measures implemented, employee training, types of cyberincidents that affect them and the costs associated with recovering from and preventing cyberincidents;

(dd) States should support businesses and communities in raising awareness of cybercrime risks, mitigation strategies and enhancing cyberpractices, as these can have significant downstream preventive benefits;

(ee) The modi operandi of contemporary cybercriminals should be carefully studied by means of intelligence analysis and criminological research in order to deploy existing resources more effectively and identify vulnerabilities;

(gg) Countries should consider specific and tailored efforts to keep children safe online. This should include ensuring domestic legal frameworks, practical arrangements and international cooperation arrangements to enable reporting, detection, investigation, prosecution and deterrence of child sexual abuse and exploitation online;

(hh) Industry is a key partner in preventing cybercrime. Countries should consider implementing mechanisms for cooperating with industry, including on referrals to competent national authorities and takedowns of harmful criminal material, including child sexual exploitation and abhorrent violent material;

(ii) Regular advisories on incident prevention should be issued and shared with users, organizations and other stakeholders to enable them to prevent cyberincidents that could potentially lead to criminal activities;

(qq) States should involve female experts in the prevention and investigation of cybercrime;

(rr) National and regional prevention experiences should be brought together to create a multilateral repository that would allow the dissemination of good practices in diverse contexts;

(tt) Greater awareness should be generated and legislative assistance should be provided on regulatory frameworks against cyberbullying and online threats of violence or abuse;

(ww) It was recommended that States invest in capacity-building to upgrade the skills of officers from the whole spectrum of the criminal justice system as an efficient preventive measure of deterrent effect against cybercrime;

(xx) UNODC should facilitate the sharing of best practices on effective and successful preventive measures against cybercrime.