Unofficial translation

Russia's comments for the seventh meeting of the Open-ended intergovernmental expert group on cybercrime
(Vienna, 6-8 April 2021)

General comments

In terms of its scope and inclusivity, the problem of the criminal use of information and communication technologies (ICTs) has long become a global threat, which affects both developing and developed countries. The criminal law mechanisms in place, some of which were developed several decades ago, and the international cooperation in the field lag far behind malicious users and cannot effectively address current challenges and threats, including due to their regional nature or limited application.

Given the circumstances, it seems that the key objective in the area is the earliest elaboration under the auspices of the UN of a convention on countering the use of ICTs for criminal purposes within the ad hoc committee established for that purpose pursuant to UN GA resolution 74/247. The new instrument seems to be another universal international criminal law instrument focused on crimes in the use of ICTs, aimed to counter them, and comprehensive in content.

Already established regional instruments and best practices of various countries of the world can be used in the drafting of this convention. It will ensure a gradual, evolutionary approach in the development of international cooperation and comprehensive support for States in need in this sphere. The Russian Federation believes it is a great opportunity to avoid excessive politicization of the negotiation process on countering ICT-related crime and translate the dialogue within the UN into practice covering criminal legal regulation.

The suggested compilation of preliminary conclusions and recommendations shows a variety of challenges faced by the UN Member States, difference in their legal systems and practical measures taken to combat ICT-related crime. Besides, it contains provisions that do not convey the exact message of the delegations' views expressed during the meetings, or are unacceptable. First of all, it concerns the preliminary conclusions and recommendations considered at the Expert Group's meeting in 2020 held in a hybrid format. The Russian delegation noted then that the Rapporteur (representative of the Netherlands) perverted the course of the discussion and paid significant attention to one regional instrument, thus having downgraded the idea of the elaboration of a universal convention. The amendment to the text made during the meeting was not reflected in the final compilation of preliminary conclusions and recommendations; that is why we expect to revert to them at the stocktaking meeting of the Expert Group.

The hybrid format of the Expert Group's stocktaking meeting complicates discussions on a rather impressive list of items, however, the Russian side expects the delegations to avoid politicization of the discussion and aim at the search for compromises and mutually acceptable solutions with a view to consolidating efforts of the international community in countering the criminal use of ICTs.

The comments on the compilation of all preliminary conclusions and recommendations are provided in Russian and English.

I. Comments on the themes of the Expert Group meetings

In our view, the provisions on the extraterritorial jurisdiction contained in para. 4 "g" of Chapter A "Legislation and frameworks" of Section II (2018) and paras. "dd" and "nnn" of Chapter A "International cooperation" of Section IV (2020) are unacceptable as they create risks of interference in internal affairs of States. These paragraphs also contradict other conclusions and recommendations of the abovementioned compilation, which focus on the need

to abide by the principles of the UN Charter, such as respect for the sovereignty of States and non-interference in their internal affairs. Such issues should be regulated by a legally binding international treaty.

Paras."a" and "c" of Chapter A "Legislation and frameworks" of Section II (2018) of the document can conflict in the part that national criminal legislation, on the one hand, can be applied to crimes committed online but at the same time cannot be applied to crimes linked to the misuse of ICTs.

In the same vein, questionable are the recommendations in paras. "n" "ii" and "iii" of Chapter A "Legislation and frameworks" of Section II (2018) on the engagement of UNODC in drafting and amending legislation, structuring ICT-related crime investigation units and providing guidance on related procedures, in terms of excessively deep interference in States' domestic affairs.

In para. 8 "q" of Chapter A "International cooperation" of Section IV (2020) the wording to the effect that private companies, notably Internet service providers, have shared responsibility in preventing and investigating malicious use of ICTs is not correct, as crime prevention and investigation fall within the purview of States' law enforcement bodies.

We cannot agree with the conclusion in para. "t" of Chapter A "Legislation and frameworks" of Section II (2018) on the 2001 Council of Europe Convention on Cybercrime (Budapest Convention) being the "best practice model" given its drawbacks, including in terms of inadmissibility of some of its provisions for the Russian Federation, and the call to join it contained also in para. "b" of Chapter A "Law enforcement and investigations" of Section III (2019).

In this regard, we note that the provisions of the Budapest Convention entrench the possibility of access of foreign competent authorities to electronic evidence outside their jurisdiction in the territory of State Parties to the Convention, which is deemed unacceptable for the Russian Federation and can be interpreted as obtaining evidence by unlawful means.

Besides, during the Expert Group meetings, the Russian delegation spoke in support of initiatives related to exploring the possibility to create special, "protected" international transmission channels for electronic requests for international legal assistance in criminal cases, as well as proposals aimed at elaborating legal rules on procedural admissibility of exchange of electronic evidence with foreign competent authorities. These issues need to be addressed not in a narrow circle with a view to imposing to the world community but in the framework of the elaboration of a relevant universal convention with all States enjoying equal rights and opportunities.

We also note that the United Nations Convention against Transnational Organized Crime (UNTOC) cannot be fully used to counter ICT-related crime as stated in paras. "u" of Chapter A "Legislation and frameworks" of Section II (2018), "k" of Chapter B "Criminalization" of Section II (2018), and "c" and "i" of Chapter A "Law enforcement and investigations" of Section III (2019), as criminals can often act alone.

We do not agree with the recommendation in para. "11" of Chapter A "International cooperation" of Section IV (2020) that any new instrument on ICT-related crime should not conflict with the existing treaties. A new international treaty can be drafted if the existing instruments in the field are outdated or irrelevant, if circumstances changed or new challenges and threats emerged, or the current realities require significant changes in the legal framework, including expansion of acts to be criminalized, increased accountability, simplified procedures for interaction, etc. These aspects are within the mandate of the abovementioned ad hoc committee, not the Expert Group.

UNGA resolution 74/247 on the establishment of an ad hoc committee to elaborate such an instrument specifically states that the elaboration of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes should take into full

consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, but makes no mention of the fact that it should not contradict them.

Subparagraph "tt" of Chapter A "International cooperation" of Section IV (2020) recommending that any elaboration of a new Convention should be handled among the experts in UNODC should be deleted. The UN ad hoc committee has been established pursuant to UN General Assembly resolution 74/247 for this very purpose, with its modalities to be determined during its first (organizational) session.

The recommendation contained in subparagraph "vv" of Chapter A "International cooperation" of Section IV (2020) regarding the start of the work of the aforementioned ad hoc committee on the elaboration of a comprehensive convention goes beyond the IEG mandate. Therefore, it would be desirable to take steps to delete this provision from the draft.

Subparagraph "xvi" of paragraph "o" of Chapter A "International cooperation" of Section IV (2020) on the establishment of an international agency for digital forensics verification and certification requires justification and further discussion as to whether such international entity needs to be established.

We believe that provisions in paragraph "b" and subparagraph "ggg" of Chapter A "International cooperation" of Section IV (2020) on the use of the Budapest Convention as a standard for capacity-building and technical assistance, as well as acquiring electronic evidence are worded in a peremptory manner. There are no standards established in this field, which is one of the reasons to create a common legal framework for cooperation pursuant to UNGA resolution 74/247.

Paragraph "l" of Chapter A "International cooperation" of Section IV (2020) concerning the so-called gender and age sensitivity is irrelevant to its content and thus can, in our opinion, be deleted.

Given that not all countries support extending and expanding the IEG mandate, we believe that subparagraphs "p" and "r" of Chapter A "Legislation and frameworks" of Section II (2018), subparagraph "o" of Chapter B "Criminalization" of Section II (2018), subparagraph "k" of Chapter B "Electronic evidence and criminal justice" of Section III (2019) and subparagraph "rr" of Chapter A "International cooperation" of Section IV (2020) should be amended accordingly to allow for a discussion for the period of the IEG operation.

The list of organizations to establish contact with or conclude an agreement with should be expanded to include other examples (CIS and the SCO) or provide no examples whatsoever to maintain the neutrality of the compilation. This particularly applies to subparagraph "b" of Chapter A "International cooperation" of Section IV (2020), where the Rapporteur distorts the nature of the discussion in a completely non-neutral manner by putting a regional instrument first. We therefore suggest that all existing regional instruments should be listed without being linked to the idea of elaborating a universal convention. One example of a successful combination of different approaches is subparagraphs "a" and "b" of Chapter A "Law enforcement and investigations" of Section III (2019).

Certain points, however, need to be clarified.

Subparagraph "a" of Chapter A "Legislation and frameworks" of Section II (2018) should specify what it means by future developments in technology that the legislative provisions of Member States should take into

account, since States are at different stages of technological development and digitalization.

The wording of the recommendation contained in paragraph "e" of Chapter A "Legislation and frameworks" of Section II (2018) is vague and should be modified, since it remains unclear what it means by saying that Member States should pursue international cooperation without requiring full harmonization of national legislation, provided that laws are sufficiently compatible to simplify and expedite the various forms of such cooperation.

Subparagraph "a" of Chapter A "Law enforcement and investigations" (2019) is inconsistent, since discussing common standards in international cooperation is not premature, as is stated in the text, but required when elaborating a universal convention, which might lead the reader to an opposite conclusion that would undermine the very idea of developing a global instrument under the auspices of the UN.

Regarding the recommendation in subparagraph "m" of Chapter B "Prevention" of Section IV (2020), it should be taken into account that developing measures to prevent the use of ICTs for criminal purposes (especially to counter illegal content) while ensuring freedom of press might be rather difficult and require additional consideration.

The term "electronic evidence" is not used in the legislation of the Russian Federation. Instead, it uses the term "digital evidence".

II. Future work of the IEG

The Russian Federation was one of the initiators for establishing the IEG and appreciates the significant role played by the Group during its 10 years of existence in discussing the issue of countering the use of ICTs for criminal purposes, as well as the importance of the draft 2013 Comprehensive Study on

Cybercrime published on the UNODC website that underpinned the further work of this negotiating platform.

The Group has considered and discussed all chapters of the draft 2013 Comprehensive Study on Cybercrime pursuant to the 2018-2021 Work Plan of the IEG adopted by consensus by the UN Commission Crime Prevention and Criminal Justice (CCPCJ), thus fulfilling its mandate.

The aforementioned Comprehensive Study notes that tackling the misuse of ICTs requires elaborating and adopting a universal convention in this field. An important step to that end was made in 2019, when the UN General Assembly adopted during its 74th session a resolution titled "Countering the use of information and communications technologies for criminal purposes". It was co-sponsored by 47 States.

The primary objective of that document is 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, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the IEG.

The Russian Federation considers this ad hoc committee another important step made by the international community in this field to move from discussing the issue of ICT-related crime and identifying the needs of States during the meetings of the IEG that has been operating for 10 years to elaborating effective measures in the form of a relevant universal convention within the framework of the aforementioned ad hoc committee.

Given the history of challenges the IEG faced in 2011-2021 due to limited resources (the Russian Federation, along with several other States, financed the meetings of the Group), as well as the conclusion of the discussion of all chapters of the 2013 Comprehensive Study on Cybercrime, we believe that the world community and relevant experts should focus on the prompt launch of the said ad hoc committee and the elaboration of a universal convention. In this context, we consider that the IEG has fulfilled its mandate and its seventh (final) meeting will be the last one.

The opportunities to discuss the phenomenon of the criminal use of ICTs and exchange best practices, however, not only remain, but are expanded through thematic discussions within the framework of annual CCPCJ sessions and a separate agenda item of the UNGA Third Committee entitled "Countering the use of information and communications technologies for criminal purposes" and introduced in 2019 pursuant to UNGA resolution 73/187, as well as the active role and openness of the UNODC, including technical assistance to States in need. During the elaboration of a universal convention, it will take some time to discuss this topic as well.

We encourage all UN Member States to take an active part in the organizational session of the aforementioned ad hoc committee (New York, May 10-12, 2020). We are convinced that it is only through joint action that the ICT-related crime can be effectively tackled.