Russian Federation

Item 6 of the agenda "Preliminary exchange of views on key elements of the draft convention"

Dear Madam Chair,

Dear colleagues.

I would like to share Russia's assessments of the key and basic elements of the future convention.

Dear colleagues, we certainly agree with the numerous speeches that the draft convention must strike a balance in matters of protecting state sovereignty, non-interference in the internal affairs of states, respect for human rights and the protection of personal data.

In our opinion, the future convention should certainly not only complement the efforts of states at the national and regional levels, but also bring international cooperation in this area to a qualitatively new level to ensure unimpeded, efficient and rapid cooperation, including real-time cooperation of law enforcement agencies of the Member States in combating the use of ICT for criminal purposes, regardless of their level of technological development.

Dear Madam Chair, now, starting from the structure of the convention already agreed upon last week in a preliminary plan, I would like to voice a number of specific provisions to fill its chapters.

General provisions. We must strictly follow the mandate of the Ad Hoc Committee determined by the UN General Assembly resolutions 74/247 and 75/282, namely, to elaborate a comprehensive convention on combating the use of ICT for criminal purposes. For the purposes of implementing the convention, it is advisable to provide a broad conceptual apparatus. In this regard, Russia proposes to include in the draft convention a section called "Use of terms", in which to explain not only what information and communication technologies, information and telecommunication networks are, but also to consider such definitions as seizure of property, malware, children's pornography, proceeds, property, information, confiscation, computer attack, digital information, critical information infrastructure, critical infrastructure facilities, ICT device, electronic evidence, and service provider. Some terminology already exists in other UN documents or regional conventions. This is done for a uniform understanding by all the participating states of the norms of the future international treaty, including considering the differences in the legislation of the states.

The issue of protecting sovereignty must be closely interlinked with the issue of jurisdiction. In particular, the convention should not confer on the competent authorities of one State Party the right to exercise in the territory of another State the jurisdiction and functions relating to the exclusive competence of that other State.

Criminalization. This chapter should bring together best practices from the international community and fill in the legal gaps that allow criminals to escape responsibility.

The convention should take into account a wide range of criminal acts. These could include such crimes committed with the use of ICTs as unauthorized access to digital information, unauthorized interception, unauthorized interference with digital information, disruption of information and communications networks, creation, utilization and distribution of malicious software, unauthorized interference with critical information infrastructure, unauthorized access to personal data, unauthorized trafficking in devices, ICT-related theft, ICT-related offences related to the production and distribution of materials or objects with pornographic images of minors, encouragement of or coercion to suicide,

offences related to the involvement of minors in the commission of unlawful acts that endanger their life or health, the creation and use of digital information to mislead the user, incitement to subversive or armed activities, terrorism and extremism-related activities, offences related to the distribution of narcotic drugs and psychotropic substances, offences related to arms trafficking, illicit distribution of counterfeit medicines and medical products, use of ICTs to commit acts established as offences under international law, infringement of copyright and related rights by means of ICTs, aiding, preparation for and attempt at the commission of an offence and other unlawful acts.

Why did Russia single out these illegal actions? They are the most dangerous and entailing the most serious consequences. We proceed from what is currently particularly relevant in the world of ICT-crime.

There is an example of crimes related to terrorist and extremist activities. Many participants have already mentioned this in their presentations. Everybody knows that that information and communication networks continue to serve for the leaders of extremist and terrorist groups a tool for recruiting new members, a means of communication and organizing terrorist actions. There is a continuing tendency to disseminate deliberately false messages, including via SMS, about terrorist attacks through electronic mail services and IP telephony to destabilize the activities of government bodies and escalate tensions in the society. Accordingly, the use of ICT by terrorists is a transnational problem, which requires coordinated responses from the world community.

Procedural issues and law enforcement. Significant attention in the convention should be given to procedural rules, as well as conditions and guarantees. The convention should have provisions regarding prompt seizure of electronic data, mutual assistance in the real-time collection of electronic information, including data on the content of messages, the prompt provision of stored technical parameters of traffic, the collection and preservation of information in electronic form accumulated and transmitted using ICT, as well as search and seizure of information.

Measures to counter crime. They should include principles and standards of conduct for service providers, raising public awareness, protecting witnesses and victims.

International cooperation. Provisions need to be made for international cooperation in extradition, mutual legal assistance in criminal matters, including asset recovery procedures, which is essential given the huge profits that perpetrators make from ICT crimes.

Regarding persons suspected of committing crimes and requested for extradition, it is necessary to fix the principle of the inevitability of punishment - **"either extradite or prosecute"** - one of the "pillars" of international criminal law cooperation, in particular in the fight against terrorism.

Russian experts concluded that often, when committing crimes using ICT, the purpose of such illegal acts is not immediate enrichment but the theft of personal data and sensitive information, i.e. user data of payment cards. To ensure the protection of personal data, it is necessary to include separate provisions on data protection in the draft convention, which would establish guarantees that ensure the protection of human rights and freedoms. Different national legal regimes for data protection should not be an obstacle to data exchange within the framework of international cooperation.

In terms of strengthening **international cooperation between law enforcement agencies**, the project should provide for emergency interaction mechanisms that qualitatively increase the speed and efficiency of work in the investigation of cross-border crimes in the field of ICTs, as well as lay a solid foundation for cooperation in such areas as: operational security of information in electronic form, prompt provision of stored technical parameters of traffic, mutual assistance in collecting technical parameters of traffic in real time, mutual assistance in collecting information in electronic form, joint investigations, special investigation methods, confidentiality and restrictions on the use of information, the creation of a network of national contact points 24/7.

Technical assistance. The project should lay a solid international legal basis for the provision of broad technical assistance to developing countries, in accordance with

their national plans and programs to combat ICT crime. Specific training programs should cover almost all areas of crime prevention, detection and investigation, as well as material support in combating crimes in the field of ICT use.

At the same time, the future document should consider the active use of modern technologies by law enforcement agencies in conducting investigations, for example, for conducting video interrogations and other procedural actions previously not available to the investigating authorities.

Reservations. The draft convention should also include provisions on the inadmissibility of reservations to some of its provisions.

Implementation mechanisms. Dear colleagues, experts understand that any multilateral international treaty without clear and transparent mechanisms for its implementation is a dead treaty. For the implementation of the Convention and the mechanisms for its review, it is advisable to provide for establishing transparent and classical mechanisms within the framework of the UN - the Conference of the States Parties. However, even the existence of such a mechanism (such conferences are usually held once every four years) in such a high-tech area as ICTs is clearly not enough. Therefore, within the framework of the Conference of the States Parties, it is necessary to have a permanent structure (for example, the UN Committee on the Exploration of Outer Space for Peaceful Purposes that has got two sub-committees, or the Commission on Narcotic Drugs - where the International Narcotics Control Board functions). We can establish an International Technical Commission (a kind of mini-GGE on ICT-crime), which could include both representatives of the participating states and relevant international and scientific organizations on a rotational basis.

Dear Madam Chair. Russia proceeds from the fact that now there is a historic chance for all of us to join forces and take a big step forward in the fight against this universal evil. We hope that the convention will make it possible to unite and direct the efforts of the world community towards the development of practical solutions in this area. At the same time, we draw attention to the fact that all the above-mentioned elements are already included in the Russian-Chinese draft convention, co-sponsored by a number of other states. In particular, it reflects the concerns of most states regarding the human rights aspect, the guarantee and protection of human rights and fundamental freedoms, the protection of personal data, which is provided for in many articles of the Russian-Chinese draft, issues of sovereignty, non-interference in the internal affairs of other states, urgent legal assistance, empowering the competent authorities with the appropriate procedural powers necessary to provide such assistance, as well as the preservation and collection of electronic evidence, and many other things that delegations spoke about previously. I emphasize that the Russian-Chinese project takes into account the provisions of

the UNCTOC, the UNCAC, the Budapest Convention and its protocols, including the Second Additional Protocol. We agree with some speakers the timeframe envisaged by the special committee's mandate for the preparation of a draft convention is extremely short. However, this should not go to the detriment of the content and quality of such an important comprehensive document, given that the convention should significantly expand cooperation between states in the field of combating cybercrime.

Thanks for your attention.