Unofficial translation

Постоянное представительство Российской Федерации при Организации Объединенных Наций

136 E 67th Street
New York, NY 10065

Permanent Mission of the Russian Federation to the United Nations

Phone: (212) 861-4900
Fax: (212) 628-0252
517-7427

Check against delivery

STATEMENT

by Deputy Director of the Department for International Information Security of the MFA of Russia Dmitry Bukin at the first session of the Ad Hoc Committee to Elaborate a Comprehensive Convention on Countering Cybercrime

10 March 2022

Dear colleagues,

I would like to take this opportunity to make some general comments now when the exchange of views on the substantive agenda items is over.

First of all, I would like to thank all my fellow Committee members for their constructive, pragmatic approach. It is obvious that at the beginning of this process many delegations presented their starting positions, and there are difficult negotiations ahead of us that will include not only cooperation on the basis of

positions of our law enforcers, but a diplomatic process as well. However, Russia believes that the Ad Hoc Committee should focus on the essential fundamental elements that derive from the mandate of the Ad Hoc Committee as stated in resolution 75/282 and the object of the convention.

1. Objectives and scope: colleagues, we are drawing up a specialized legal treaty, not a human rights convention. A reasonable balance must be struck human rights provisions and the view firmly expressed by dozens of delegations regarding national sovereignty, territorial integrity, and non-interference in internal affairs, which is reflected in the Russian-Chinese draft convention. Most of its articles, especially those on electronic data, refer to the need to respect human rights. We must protect the rights and property of our citizens from cyber criminals through the mechanisms of the convention and not to protect our citizens from the mechanisms of the convention.

As for the scope, one might say that some delegations did not vote for resolution 74/247 on the elaboration of a convention on countering specifically the use of ICTs for criminal purposes. However, resolution 75/282 that was adopted just six months ago and clearly concerned ICTs, was adopted by consensus, so Member States that are now advocating the reduction of the scope to only computer crimes agreed with such scope.

The same applies to the proposal to exclude the offences that are already covered by existing international instruments against crime. We checked: the UNTOC does not say a word about the use of ICTs, while it is clearly an aggravating factor for conventional crimes, bearing in mind the speed at which crimes are committed and the anonymity of criminals.

2. Some delegations proposed to exclude the private sector from the scope of the convention. It sounded ambiguous: legal entities were mentioned, with no extension to the private sector.

Communications companies and service providers will play a key role in the implementation of the convention. How will law enforcement be able, for example, to freeze electronic evidence if private providers are not bound in any way? It is the private business that determines the speed and success of investigations.

It is particularly telling that this was proposed by the countries that are Parties to the Budapest Convention. Let me remind you that under the second additional protocol to this convention, communications operators and Internet service providers bear a high responsibility for providing data and assistance to law enforcement agencies. During the drafting of the text of the second additional protocol, it was explicitly stated that the instrument will not work without business sector.

Therefore, we not only fail to strengthen international cooperation, as we point out in the "Objectives and the scope of the convention", not only fail to complement the existing level of international interaction, as pointed out by several delegations, but we will also weaken the level of cooperation in a universal convention as compared to regional instruments.

3. If you solve the puzzle by gathering the speeches of several delegations – who required a brief convention and said that it is necessary to narrow its scope, not to try to criminalize the ICT component of the existing elements of crime in the international instruments, not to touch the private sector, but to use technologically neutral terminology – then you shall see that this puzzle takes the form of a framework convention. Do we need such a framework instrument? I do not think so. Our citizens and businesses need a practical mechanism for preventing and combating cybercrime and its consequences. Do we wish to create such a mechanism or instrument that goes straight to the UN library just as an item?

There are examples of effective bilateral cooperation in the fight against cyber-evil. Just recently, hacker groups in Russia that were causing serious damage to entire industries in another country were detained. But such bilateral interaction depended on the political will of the two governments and the current political situation. Our task is to create a legally binding mechanism for 24/7 coordination of operational activities among our law enforcement agencies, which would not depend on the political situation by definition.