CONCEPT NOTE

Why does Russia consistently advocate for the inclusion in the future convention of provisions on countering the use of information and communications technologies (ICTs) for terrorist and extremist purposes?

Majority of domestic terrorism cases involve, to some extent, the use by perpetrators of the Internet. However, the national legislation of many developing countries, unlike the developed ones (Australia, Great Britain, European Union, USA, New Zealand, etc.), is not sufficiently advanced in this area. Therefore, with a view to prosecute terrorists competent authorities of such states apply their criminal provisions related to other crimes. That is not about combating the current threats adequately.

Terrorist groups are taking their work in the Internet to a new level. In particular, ISIS has used a powerful media holding in its structure that produced a wide range of media products: video propaganda, films, audio recordings of sermons, electronic versions of magazines, booklets, posters, etc. To these ends, the terrorist organization employed its own Internet resources, as well as numerous accounts on the most popular social networks (*Facebook, YouTube, Instagram,* etc.).

Internet resources are also actively used for organizing and preparing terrorist attacks. Thus, a series of terrorist attacks which took place in France in 2015 and 2016 were coordinated through the Telegram messenger. There were similar cases in Indonesia and Sweden in 2017.

The ICTs were also largely used for the preparation and coordination of terrorist attack, in particular in Indonesia in 2021, Turkey in 2022 and in Russia in 2023.

Terrorists tend to use cryptocurrencies, various “electronic wallets,” mobile banking and crowdfunding for financing their own activities. All of these significantly complicate the task of cutting off channels of financing of terrorist groups. At the same time, experts highlight such a way of terrorism financing in the Internet as creation of charity organizations to collect donations.

Online games and the Internet entertainment industry are becoming an important platform for terrorist organizations (it is employed by extremists for the promotion of their ideology and recruitment of vulnerable people).

The issue of collecting and storing electronic evidence of terrorist crimes is also acute. Law enforcement agencies of most countries, especially of the developing ones, lack qualified personnel able not only to identify, but also to investigate crimes of terrorist groups in information space. Not all terrorist actions fall under legislation, neither the necessary evidence could be obtained from other states. Often such requests cannot be fulfilled because of gaps in the domestic legislation or the data has already been deleted.

Experts draw special attention to the elaboration by terrorists of their own artificial intelligence samples (there were several versions of the chatbot ChatGPT created without restrictions on content generation).

In this regard, states have started elaborating documents and mechanisms to counter terrorist activities in information space at the global and regional levels. The UNGA resolution 74/247 on elaboration of a first ever comprehensive convention was adopted on Russia's initiative and got large support from Member States. Our primary task is to present during the 78th UNGA session such a document that would ensure effective international law enforcement cooperation in countering the use of ICTs for criminal purposes.

Global level

The UN Security Council resolution **1617 (2005)** expressed concern over the use of various media, including the Internet, by terrorist organizations and their associates, including for terrorist propaganda and inciting terrorist violence.

In its resolution **1624 (2005)** the UN Security Council recognized the importance that, in an increasingly globalized world, States act cooperatively to prevent terrorists from exploiting sophisticated technology, communications and resources to incite support for criminal acts.

The UN Security Council resolution **2161 (2014)** expressed concern at the increased use, in globalized society, by terrorists and their supporters, of new information and communications technologies, in particular the Internet, to facilitate terrorists acts, as well as their use to incite, recruit, fund or plan terrorist acts.

The UN Security Council resolution **2178 (2014)** expressed concern over the increased use by terrorists and their supporters of communications technology for the purpose of radicalizing to terrorism, recruiting and inciting others to commit terrorist acts, including through the internet. It underlined that the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts and condemned violent extremism, which can be conducive to terrorism.

Moreover the document clearly calls upon Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist act.

The UN Security Council resolution **2354 (2017)** shouldered the primary responsibility for countering terrorist acts and violent extremism conducive to terrorism on Member States. It underlined that terrorism can only be defeated by a sustained and comprehensive approach involving the active participation and collaboration of all States and international and regional organizations to impede, impair, isolate, and incapacitate the terrorist threat. It also noted with concern that terrorists craft distorted narratives that are based on the misinterpretation and misrepresentation of religion to justify violence, which are utilized to recruit supporters and Foreign Terrorists Fighters, mobilize resources, and garner support from sympathizers, in particular by exploiting information and communications technologies, including through the Internet and social media.

The UN General Assembly resolution **77/298** reiterated the obligation of Member States to prevent and suppress the financing of terrorist acts and refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by stemming recruitment of members of

terrorist groups, and to criminalize the willful provision or collection, by any means, directly or indirectly, of funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out a terrorist act, and expressed concern over the misuse of the Internet and other information and communications technologies, including virtual assets, mobile payment systems and crowdfunding, and other forms of terrorism financing.

This document also expressed deep concern of the UN General Assembly by the use of the Internet and other information and communications technologies, including social media platforms, for terrorist purposes, including the continued spread of terrorist content, and encouraged Member States to work together.

Regional Level

Commonwealth of Independent States (CIS)

The 2019 Strategy of Ensuring Information Security of the CIS State Parties expresses the need to form mechanisms for international cooperation in the field of countering the threats of the use of information and communications technologies for criminal and terrorist purposes, as well as to increase the effectiveness of international cooperation in the field of combating information crime and information terrorism.

The 2018 Agreement on Cooperation Among the Member States of the CIS in the Fight Against Crimes in the Field of Information Technology provides for the obligation of the Parties to establish, in accordance with national legislation, as a criminal offence, if committed intentionally, distribution of materials recognized in accordance with established procedure as extremist or containing calls for terrorist activities or justification of terrorism with the use of the information and telecommunications network "Internet" or other channels of electrical communication.

OSCE

The OSCE has accumulated a solid corpus of political commitments in the context of figthing terrorism, in particular those contained in the Ministerial Council Decision No. 3/04 on combating the use of the Internet for terrorist purposes, Ministerial Council Decision No. 7/06 on countering the use of the Internet for terrorist purposes and Ministerial Council Decision No. 5/07 on public-private partnerships in the fight against terrorism.

The Joint Statement of the Ministers of Foreign Affairs of Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan "On preventing and combating the use of the Internet for terrorist purposes" delivered at the 28th OSCE Ministerial Council meeting (Stockholm, 2 December, 2021) expresses serious concern about the increasing use of the Internet for terrorist purposes, including live broadcasts of terrorist attacks. It is noted that information and communications technologies, including the Internet and social networks, are used to recruit new supporters and Foreign Terrorist Fighters as well as to mobilize resources. Concern is expressed about the spread, including through the Internet, of hate speech and ideas that incite violence and fuel terrorism.

ASEAN

ASEAN Regional Security Forum (ARF) adopted in 2019 a Statement on Preventing and Countering Terrorism and Violent Extremism Conducive to Terrorism. It expresses concern that terrorists continue to use information and communications technologies, particularly the Internet and social media, for terrorist purposes, including commission, inciting, radicalizing and recruiting, financing or planning of terrorist attacks. The document also urges ARF Participants to focus on online platforms in order to promote their efforts to prevent the streaming, downloading or re-uploading of a terrorist content and content related to terrorism and extremism.

Therefore, the abovementioned documents of a universal and regional nature clearly demonstrate the need for a mechanism for countering the use of

information and communications technologies for terrorist and extremist purposes to be regulated in the text of the convention under elaboration. Nothing but detailed legal regulation of this issue will allow Member States to carry out an effective international cooperation in the fight against terrorist and extremist crimes.