Legal framework and experience of the CIS member states in countering disinformation emanating from terrorist and extremist organizations

Alexander Smirnov,
Executive Secretary of the Scientific and Advisory Council at the Anti-Terrorist Center of the CIS member states

Good afternoon, dear participants of the expert meeting! My name is Alexander Smirnov, I represent the Anti-Terrorist Center of the member states of the Commonwealth of Independent States. Our Center is a specialized sectoral body of the CIS and is designed to ensure coordination of interaction between the competent authorities of the CIS member states in the field of combating international terrorism and other manifestations of extremism. The Commonwealth of Independent States currently includes 11 states: Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan and Ukraine.

Before I proceed with the keynote speech, I would like to thank the office of the OSCE Representative on Freedom of the Media and personally Andrei Richter for the invitation to such a representative event. This is a great opportunity for us to hear the positions of European experts on countering information risks and share the positive experience of the Commonwealth of Independent States in this area.

Today we are discussing the topic of disinformation and fake news. These threats as such are by no means new. On the contrary, disinformation has always been considered a classic tool of psychological warfare. For example, Alexander the Great often used tactics that involved spreading false rumors about the superior numbers and power of his troops. Another classic example is the deception operation employing a Trojan horse, carried out by the Greeks to take Troy. All these events took place before our era.

However, in present-day conditions, the threat of spreading false information has gained special prominence. There are several reasons for this, but they are all related to the development of new information and communication technologies and their impact on society.

First, the development of global broadcasters and the Internet has made a truly

cross-border dissemination of information a reality.

Secondly, the development of social Internet technologies (Web 2.0) has empowered the users to broadcast information to a wide audience (that is, endowing them with mass media functionality), thereby multiplying the number of mass media outlets.

Third, new algorithms for tracking user behavior have enabled personalized news feeds that display information that matches the views of the recipient, and filters out the contradicting information. The researched dubbed this phenomenon a "filter bubble".

Fourth, there have been major changes in the social psychology of the mass media audience, with the scholar heralding the "post-truth era." In post-truth conditions, the public opinion is more shaped by messages that appeal to the emotions and personal beliefs of the audience, rather than by the truth and objective facts.

The above drivers led to the widespread dissemination of fake news in the new digital environment. New potential for disinformation is created by artificial intelligence technologies, in particular, those creating the so-called deepfakes.

Therefore, we believe the international community's close attention to the threat of disinformation to be quite justified. At the same time, I would like to make a few reservations for a correct understanding of the subject field. First, disinformation is not an isolated phenomenon, but rather a wide range of types of communication, which are based on the purposeful transmission of false information. Therefore, disinformation should, firstly, be considered along with other types of destructive communication within the framework of the general subject field of information security; and secondly, be studied in the diversity and multitude of its manifestations.

Disinformation can manifest itself in different contexts: as an element of an information war between states, as an instrument of destructive propaganda, as a form of destructive interpersonal communication. Accordingly, the tools and methods for combating fakes should be flexible and variable, especially with regard to mass media. Here, the “graduated and differentiated approach” proposed by the Council of Europe to the regulation of new media would be very appropriate.

In addition, one mustn't but note the extreme politicization of the topic of disinformation, which significantly distorts the perception of the manifestation of this threat. We constantly see how some countries of the world focus on some false messages, while totally oblivious to the others. Attempts are being made to label certain states and mass media as permanent sources of fake news. Such policy is counterproductive and impedes the development of common approaches to respond to a threat common to world's nations.

When we consider the threat of misinformation from terrorist and extremist organizations, we include a number of aspects.

The first and most obvious of these is the k*nowingly false reporting of an act of terrorism*. This action is recognized as a crime in the CIS countries. As a rule, the perpetrator reports over the phone about a planted explosive device and their intention to trigger it. Such actions are often performed by mentally sick people, as well as adolescents seeking to "pull a prank". Although terrorists can also be the subjects of false messages, thus probing the readiness of the authorities or diverting their attention from the true targets of attacks. The danger of this crime lies in the fact that it harms public safety, undermines the normal life of society, significantly disrupts the work of state bodies, companies, organizations, and transport.

However, in recent years, *mass (fanned) distribution of false bomb threats* has become more widespread. Thus, in Russia, in just a few months of 2019, there were reports of more than 16 thousand false bombing threats targeting social infrastructure, including schools, kindergartens, hospitals, and transport facilities. Distribution was done via secure e-mailing and VoIP services with anonymizer functionality, which speaks of the professionalism and purposeful nature of subversive activities. Similar cases were reported in other countries of the Commonwealth, in particular in the Republic of Belarus.

The next block of disinformation risks is associated with the propaganda and recruitment activities of terrorist and extremist organizations. When broadcasting their propaganda of hatred and enmity, extremists often use *false narratives* that distort the meaning of religious teachings and scriptures. The difficulty in neutralizing the narratives of extremist propaganda is that it is often based on

mythology, which is very difficult to disavow by means of rational arguments. Radicals are susceptible to myths of a religious nature (they permeate the ideology of jihadists) and conspiracy theories (for example, the myth of the "global Zionist conspiracy" among neo-Nazis).

Techniques of deception and manipulation of the mind are actively used when terrorists recruit new members. The recruitments of supporters is carried out both via interpersonal communication and in the course of group communication across numerous virtual communities on social media and messengers. Moreover, in these closed virtual groups of like-minded people, radical ideas are amplified through mutual reinforcement (echo chamber effect).

The Anti-Terrorist Center of the CIS member states is studying the positive experience of the competent authorities of the Commonwealth member-states in countering the destructive information activity of terrorist and extremist organizations, including disinformation.

The legal basis for the activities of law enforcement agencies in this area is formed by international legal instruments and national legislation in the field of combating terrorism and extremism. Within the framework of the Commonwealth of Independent States, a number of important documents have been adopted in this area, including the Agreement on Cooperation of the CIS Member States in the Fight against Terrorism of 1999, the Concept of Cooperation of the CIS Member States in the Fight against Terrorism and Other Violent Manifestations of Extremism in 2005, the Agreement on Cooperation of CIS Member-States in the Field of Information Security in 2013, as well as a package of model laws. A number of significant practical measures to counter information threats of an extremist nature are enshrined in the CIS interstate programs to combat terrorism and other violent manifestations of extremism. Currently, a program for 2020-2022 is being implemented.

The use of disinformation in the activities of terrorist and extremist actors is countered in the Commonwealth countries within the following main areas:

1. *Criminalization of the most dangerous forms of disinformation and holding the perpetrators legally accountable*: means the establishment of criminal and administrative liability for the dissemination of certain types of disinformation. As a

rule, social dangerous consequences resulting from such disinformation are a mandatory characteristic of such *corpus delicti*. Above, we talked about the criminalization of knowingly false reporting of acts of terrorism. In 2019, Russia introduced administrative liability for the dissemination of fake information in the media and information and telecommunication networks. At the same time, the state has provided a legal definition of fakes as deliberately unreliable socially significant information, disseminated under the guise of reliable messages, posing a threat to the life or health of citizens, property, public order and public safety. It is punishable by fine (both for individuals and legal entities), the amount of which depends on the severity of the consequences.

2. *Securing legal prohibitions and restrictions on the dissemination of false information in the media and on the Internet*: acknowledging the internationally recognized principle of freedom of the media, the national legislation of the Commonwealth countries sets certain limits and restrictions. In particular, the Russian law on the media establishes the inadmissibility of abuse of freedom of the media. The distribution of materials containing public calls for terrorist activities or publicly justifying terrorism, other extremist materials, and other information prohibited by law is classified as a form of such abuse. This also includes fake news. A similar restriction is enshrined in the Russian law "On Information, Information Technologies and Information Protection". Compliance with legal restrictions is monitored by a dedicated agency — Roskomnadzor.

3. *Restricting access to extremist content and false messages on the Internet*: in the countries of the Commonwealth, legal algorithms have been established to limit access to illegal content, including extremist materials. In recent years, attempts have been made to include fake messages in the scope of these algorithms. This has already been done in the Russian Federation, similar is being discussed in the Republic of Belarus. The decision to restrict access to illegal content can be made by both judicial and administrative authorities with the possibility of judicial appeal against the latter. These mechanisms have proved successful, while, of course, not creating a sterile digital environment.

4. *Explanatory and counter-propaganda efforts offline and in digital environment*: the law enforcement agencies of the Commonwealth countries have

come to a clear understanding of the impossibility of overcoming the destructive information activity of extremists by only prohibitive measures. In this regard, they, in cooperation with other state agencies and civil society, are doing a lot to inform about the social danger of terrorism and extremism, the possible forms of their manifestation in the digital environment, to expose the false ideological narratives of extremists and offer alternative positive ideas. Awareness-raising is of particular importance for combating fakes, since they spread like wildfire across social networks and instant messengers. Therefore, a quick and efficient response is critical. Moreover, unlike broad preventive anti-extremist measures, where public institutions play a key role, neutralizing fakes requires quick and clear reaction of the governmental press services and delivery of reliable information through the media and other available channels.

5. *Increasing media literacy and building cybersecurity culture*: neither external filters, nor the most effective work of public institutions can completely neutralize the flow of fake information and other negative content. In this regard, the formation of critical thinking and other media literacy competencies at the end link of the information chain — the consumer of information — is of great importance. It is a universal tool for protection against any information threats, the value of which can hardly be overestimated. In addition to a wide range of training activities, the Commonwealth countries are introducing corresponding topical modules into the school curricula. Educational activities to foster cybersecurity culture are also carried out by IT flagships, such as Yandex and Kaspersky Lab.

Concluding my speech, I would like to note the following. The digital environment will continue to generate new risks and modify existing threats as it evolves. Response requires a concerted approach and collaborative effort to effectively address cyber threats while respecting fundamental human rights. Local measures in the context of the global information space will certainly fall short. In this regard, it is important to implement the initiatives proposed by the Russian Federation and supported by many countries of the world community for the adoption of universal international treaties in the field of international information security and the fight against crime and terrorism in the information domain.