THE PHENOMENON OF TERRORISM IN THE INFORMATION SPACE

Usarov Gayrat Kadyrovich
Position: Senior lecturer, Place of work: Higher Military Aviation School of the Republic of
Uzbekistan. Department of Socio-Economic and Humanitarian Disciplines

Annotation
The article examines the phenomenon of terrorism in modern conditions and current problems related
to this problem, which affect a wide range of not only private and corporate interests, but also threaten
the national security of the country. The main trends in the development of information threats in the
modern global information space and the measures necessary to neutralize them are outlined.

Keywords: phenomenon of terrorism information terrorism, information threats, national security,
information security, global information space, terrorism.

Introduction
The problem of terrorism at the turn of the XX — XXI centuries has acquired threatening proportions.
And this seems natural against the background of the globalization of violence in recent years. The mass
media regularly reproduces reports of terrorist acts committed in various parts of the globe. The tone
of these messages is dominated by the spirit of sensationalism and high emotionality. On the one hand,
they express a thirst for uncompromising struggle and just retribution against terrorists, on the other -
a sense of uncertainty, powerlessness of the authorities, underlying fear and hopelessness. Naturally,
all this information quite adequately creates in the masses a sense of a serious threat to security from
terrorists.
Currently, terrorism is one of the most serious problems of human security, being the quintessence of
modern violent crime. Terrorism occupies a leading place among the threats to the national security of
the country today.
The activities of terrorist organizations are of a cross-border nature, they are "impersonal" and pose a
danger not to a particular person or country, but are a global problem of the entire civilization. For
terrorist organizations, terror is a way of life and the meaning of existence, and therefore the fight
against it must have a multifaceted character. It is necessary to note the increasing variety of ways of
carrying out terrorist activities aimed at the emergence of interethnic and interfaith conflicts, the main
purpose of which is to destabilize the situation in society, intimidate the population, provoke military
conflicts, and ultimately the redistribution of power or the destruction of the territorial integrity of the
state.
In the XXI century, the whole world has entered the era of globalization, which has become possible
not only due to the elimination of economic national barriers, accompanied by cheaper technical
achievements and communications, but also due to the increasingly exciting process of computerization
of society, when telecommunications acquire an exceptional role. A new era has come – the era of

"digital information", which resulted in the emergence of a new way of carrying out terrorist activities - information terrorism.

Currently, almost all computer means of creating, processing, transmitting and storing information are easily vulnerable to terrorists. Banking, stock exchange, archival, research, management systems, the Internet, means of communication from satellites to smartphones, electronic mass media, publishing complexes, various databases of personal data – all this can be attacked with the appropriate qualification of a terrorist from a single computer.

Information terrorism is a fairly well-mastered forms and methods of actions used to solve a fairly wide range of tasks, both local and strategic. A particular danger in the current conditions is the use of a significant level of information development of the state for purposes not aimed at the common good. Information terrorism is a threat to the security of mankind, comparable to nuclear, bacteriological and chemical weapons, and the degree of this threat, due to its novelty, does not have a sufficiently precise characteristic.

Information terrorism is a clear and purposeful impact on computer information, systems, programs and data, as well as computer networks, aimed not at the physical destruction of people and the elimination of material values, but at destabilizing public order, large-scale disruption of communication networks and systems, imposing their will on power structures. Information terrorism is characterized by anonymity, a high degree of latency and the relative ease of carrying out terrorist acts. Law enforcement agencies are particularly concerned about the activities of terrorist organizations related to the use of the global Internet, from which open sources it is possible to obtain information about the technology of manufacturing explosives, biological, chemical and even nuclear weapons of terrorists, as well as tactics of terrorist acts.

Terrorist acts in the information space can be committed not only by individuals or terrorist groups, but also by one State against another. In this regard, information terrorism is no different from any other type of terrorism. Extremist groups, separatist forces, preachers of ideas that contradict universal values, intensively use modern technologies to promote their ideology and conduct information wars.

To combat information terrorism, it is necessary to create an effective system of interrelated anti-terrorist measures aimed at protecting information resources from misuse and unauthorized interference.

One of the most important circumstances determining the success of prevention, detection and suppression of possible manifestations of information terrorism in a State governed by the rule of law is the creation of adequate socio-political and criminal situation in the country of national anti-terrorist legislation based on generally recognized by all States anti-terrorist principles. The system of legal regulation of information security consists of a set of legal norms regulating relations in the field of information protection, legal relations arising on the basis of the application of relevant legal norms, and relevant law enforcement acts.

Taking into account the indisputable need for legislative regulation of information security, in Uzbekistan in 2000, the President of Uzbekistan signed the Law of the Republic of Uzbekistan on combating terrorism [1] and the decree of the President of the Republic of Uzbekistan on the approval

of the national strategy of the Republic of Uzbekistan on countering extremism and terrorism for 2021-2026 [2] which, in fact, is the legal regulator of information protection in Uzbekistan.

It should be noted that the formation of the legal basis for information security has begun in Uzbekistan today. Also, work is currently underway to create mechanisms for the implementation of the right to ensure information security, the development and preparation of draft laws regulating public relations in the information sphere, measures are being taken to ensure information security in public authorities, local public authorities, enterprises, institutions and organizations, regardless of the form of ownership, and, as far as possible, familiarization of the population with the basic principles of information security. In addition, the information security of Uzbekistan is promoted by the state system of information protection, the system of protection of state secrets, the system of licensing activities in the field of protection of state secrets and the system of certification of information security tools.

Despite all of the above, the state of information security in Uzbekistan leaves much to be desired. The level of legal protection of information resources does not correspond to the prevailing needs of the population, as well as the information and technological progress that is constantly gaining momentum.

It is possible to correct the current situation only with the appropriate legislative consolidation of information security provisions by an array of regulatory legal acts. It is necessary to give a clear legal description of such categories as "information terrorism", "information war", "information weapons", etc. To do this, it is necessary first of all to ensure the purposeful activity of all state bodies and public organizations on existing aspects of information security.

References

1. Ўзбекистон Республикасининг "Терроризмга қарши кураш" тўғрисидаги қонуни, 2000 йил - 20 модда.
2. 2021 — 2026 йилларга мўлжалланган экстремизм ва терроризмга қарши курашиш бўйича Ўзбекистон Республикаси миллий стратегиясини тасдиқлаш тўғрисидаги фармони, 2021йил. – § 5-6.
3. Мирзиёев Ш.М.Янги Ўзбекистон стратегияси ,Тошкент, 2021йил-7 боб.
4. Салимов К.Х. Региональные конфликты и международный терроризм. Проблемы урегулирования региональных конфликтов в современных условиях. - М., 1991.