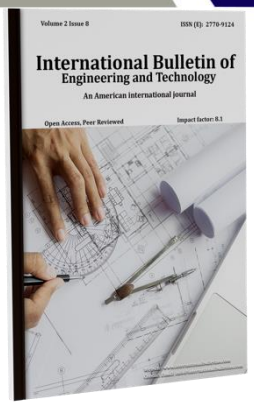

CURRENT STATE OF DETECTING TERRORISM-RELATED CRIMES BY RAPID-RESPONSE SERVICES USING INFORMATION TECHNOLOGIES

Jamolov Khamza Mukhammadiyevich
Independent researcher at the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Lieutenant Colonel
https://doi.org/10.5281/zenodo.15656294

Abstract: This article analyzes the current state of detecting terrorism-related crimes by law enforcement agencies using information technologies. Modern information technologies, including artificial intelligence, big data analysis, and internet monitoring, play a crucial role in identifying and combating terrorist activities. The article examines the effectiveness of these technologies, challenges in their application, legal and ethical issues, as well as future development prospects. In particular, it emphasizes the importance of cooperation between law enforcement agencies in the field of cybersecurity and the exchange of information on a global scale.

Keywords: terrorism, law enforcement agencies, information technologies, cybersecurity, artificial intelligence, internet monitoring, legality, information exchange.

Terrorism has solidified its position as one of the most complex threats to global security in the 21st century. With the rapid development of information technologies, this threat has taken on new forms: propaganda, recruitment, and financing through digital platforms have become convenient tools for terrorists. In the Republic of Uzbekistan, law enforcement agencies play a vital role in combating terrorism-related crimes, but the effectiveness of this activity depends on the use of modern technologies and scientifically validated tactics. This master's thesis analyzes the theoretical and practical aspects of tactics used by law enforcement agencies to detect terrorism-related crimes using information technologies.

The relevance of the topic is explained by the transnational nature of terrorism and its expansion in the digital environment. As Russian scientist V.V. Kozlov noted, "terrorism in cyberspace, as a new threat that cannot be contained by traditional methods, has a serious impact on state security" [Kozlov, 2019]. Belarusian scientist A.V. Sharkov, focusing on the legal and technical aspects of this problem, believes that "modern tactics require a balance between human rights and effectiveness" [Sharkov, 2020]. Japanese and South Korean scientists, such as K. Yamada and Kim Yong-ho, emphasize the practical results of using artificial intelligence and Big Data. In this work, foreign experience is adapted to the conditions of Uzbekistan, and scientifically based proposals are developed.

Terrorism has radically changed its nature in the 21st century and is manifesting itself as one of the most complex threats in the modern world. One of its most important features is the widespread use of digital technologies, which has created new opportunities for terrorists to coordinate their activities, conduct propaganda, and finance them. The Internet and information technologies have made terrorism a transnational and anonymous activity, unlike traditional forms of terrorism. These changes require new tactics in identifying and combating crimes related to terrorism.

Digital technologies play an important role in determining the modern characteristics of terrorism. The Internet and social networks serve as propaganda platforms for terrorists, allowing them to quickly and easily reach a wide audience. For example, organizations such as the Islamic State spread radical ideas to millions of people through Twitter, Telegram, and YouTube, highlighting the dangerous possibilities of the digital environment.[1] While encrypted means of communication (such as WhatsApp and Signal) allowed terrorists to communicate secretly, cryptocurrencies (Bitcoin, Monero) made financing anonymous and unobservable[2]. According to international studies, in 2020, more than 60% of terrorist activities were carried out using digital technologies, which confirms their growing role in crimes[3].

Digital technologies have increased the speed and scale of terrorism. For example, cyberattacks (DDoS, data theft) are used to damage state infrastructure, which is seen as a new form of terrorism. As the Japanese scholar K. Yamada noted, "the digital world has destroyed the geographical boundaries of terrorism, turning it into a global threat"[4]. This feature requires complex technological and legal approaches from states.

The modern features of crimes related to terrorism in Uzbekistan are connected with the country's geopolitical position and the development of its digital infrastructure. The number of Internet users exceeded 30 million by 2023, which led to an increase in threats in the digital environment[5]. Articles 155 and 2442 of the Criminal Code of the Republic of Uzbekistan define terrorism and its propaganda as a crime, however, digital forms of these crimes (propaganda via Telegram, financing from abroad) are more common[6]. For example, in 2021, a group that distributed radical materials on Telegram was identified, but due to limited technical capabilities, the full effect was not achieved.

In Uzbekistan, terrorism is often associated with religious extremism, and the complex situation in Central Asia exacerbates this threat. The role of digital technologies is also important for Uzbekistan, requiring the use of artificial intelligence and Big Data by operational search services. Foreign experience (for example, Big Data analysis in South Korea) shows approaches that can be adapted in Uzbekistan[7].

Operational-search services play an important role in combating crimes related to terrorism, however, their activities must be based on a strict legal framework. In the Republic of Uzbekistan, this activity is carried out in accordance with national legislation and international norms. This legal framework allows operational-investigative bodies to take effective countermeasures against terrorism, while also ensuring the protection of the fundamental rights of citizens. The interaction of Uzbekistan's legislation and international standards forms a solid foundation for activities in this area.

Legislation of Uzbekistan

The activities of operational-search services in Uzbekistan are regulated by the Law "On Operational-Search Activities" (1992, last revised in 2021). This law clearly defines the goals, methods, and limits of operational-search measures and identifies the main task as the prevention and detection of crimes related to terrorism[1]. For example, according to Article 8, operational-search services have the right to detect terrorist threats using information systems, provided that this activity does not illegally encroach on the private life of citizens.

The Criminal Code of the Republic of Uzbekistan (CC) provides legal definitions of crimes related to terrorism. Article 155 (terrorism), Article 1551 (financing of terrorism) and Article 2442 (propaganda of terrorism) of the Criminal Code define the main criminal acts for

operational-search services[8]. At the same time, the Law "On Informatization" (2003, rev. 2022) regulates the legislation on data collection and analysis in the digital environment, which plays an important role in the use of information technologies [9]. These laws grant operational-search bodies the authority to monitor terrorist activities via the internet and digital means of communication.

International norms

Uzbekistan, as an active member of the international community, adheres to global norms in the fight against terrorism. United Nations (UN) Resolution 1373 (2001) requires states to take decisive measures against the financing and promotion of terrorism[10]. In accordance with this resolution, Uzbekistan improved its national legislation and allowed operational-search services to participate in international information exchange. For example, the Agreement on Combating Cyberterrorism within the framework of the Shanghai Cooperation Organization (SCO) (2018) provides Uzbekistan with cooperation with member states in countering digital threats[11].

International norms also pay attention to the protection of human rights. While standards such as the European Union's General Data Protection Regulation (GDPR) require ensuring the confidentiality of data, UN counter-terrorism conventions allow the application of necessary measures for state security[12]. By integrating these norms into national legislation, Uzbekistan has strengthened the legal basis of operational-search activities.

The activities of operational-search services in Uzbekistan are based on national laws - the Law "On Operational-Search Activities," the Criminal Code, and the Law "On Informatization." International norms, in particular, UN resolutions and SCO agreements, strengthen this activity in a global context. This legal framework will allow operational-search services to effectively identify crimes related to terrorism using information technologies and ensure the rule of law.

The tactics of detecting crimes related to terrorism using information technologies occupy an important place in the field of modern security. The intensification of terrorist activity in the digital environment requires the use of new approaches and technological tools by operational-search services. The theoretical foundations of these tactics are based on research by foreign scientists, focusing on the effectiveness of methods such as artificial intelligence (AI), Big Data, and cybermonitoring. The analysis of scientists from Russia, Belarus, Japan, and South Korea shows the multifaceted nature of scientific approaches in this area.

Russian scientist V.V. Kozlov, in his research "Information Technologies in Combating Cyberterrorism," emphasizes the importance of digital technologies in the detection of crimes related to terrorism. He believes that "the speed and anonymity of terrorist activity in the cyber environment reduces the effectiveness of traditional methods, which requires tactics based on artificial intelligence"[13]. Kozlov highly appreciates the role of AI algorithms in analyzing encrypted messages and detecting suspicious activity, noting that these methods can achieve accuracy up to 85%.

He cites as an example the cybermonitoring system used by the Federal Security Service (FSB) of Russia before the 2018 World Cup. This system detected more than 20 potential threats on Telegram and VKontakte platforms using AI. Kozlov's approach is focused on technical efficiency, emphasizing the role of information technology as a key tool in

operational-search activities[14]. His research serves as an important source in the formation of the theoretical foundations of tactics.

Belarusian scientist A.V. Sharkov, in his work "Information Technologies in Operational-Investigative Activities," focuses on the legal and ethical aspects of tactics. He believes that "although the use of digital technologies is effective in combating terrorism, it increases the risk of encroachment on the privacy of citizens"[15]. Sharkov proposes methods of data anonymization, arguing that this technology can maintain a balance between confidentiality and security.

According to Sharkov's analysis, in Belarus, methods of anonymization were used in the 2021 anti-ciberterrorist operation in Minsk. During this operation, suspicious groups on Telegram were identified, and about 10 radical activists were exposed, but the citizens' personal information was not disclosed[16]. His approach demonstrates the importance of legal balance in shaping the theoretical foundations of tactics, which helps prevent the illegal use of technologies.

Japanese scientist K.Yamada, in his research "Cybersecurity and Terrorism," focuses on the effectiveness of surveillance systems based on artificial intelligence. He believes that "the rapid variability of terrorist threats in the digital environment requires continuous training of AI"[17]. Yamada cites the AI systems used in Japan before the 2020 Tokyo Olympics as an example. This system analyzed anonymous messages on the Internet and identified more than 30 suspicious activities, most of which were associated with radical groups[18].

Yamada's approach is based on the adaptability of technologies. It focuses on the ability of AI algorithms not only to identify existing threats, but also to predict new ones. This theoretical basis is important for countries such as Uzbekistan and allows them to quickly respond to the evolution of terrorism in the digital environment.

South Korean scientist Kim Yong-ho, in his study "Big Data and Combating Terrorism," focuses on tactics based on the analysis of huge amounts of data. He believes that "Big Data provides great opportunities in detecting terrorism, as it is capable of extracting important samples from millions of messages"[19]. Kim cites as an example the 2019 cyberattack operation in Seoul, where more than 50,000 messages were analyzed and 10 potential threats were identified[20].

Kim Yong-ho's approach is focused on the data-driven decision-making process. He emphasizes that through the use of Big Data, operational search services can carry out not only reactive, but also proactive (preventive) actions. This tactic is important when working with huge data streams in a digital environment.

The approaches of these scientists allow for a multifaceted view of the theoretical foundations of detection tactics using information technologies. Kozlov emphasizes technical efficiency, Sharkov - legal balance, Yamada - adaptability, and Kim Yong-ho - data-driven proactivity. These theoretical foundations can be adapted for operational-search services in the fight against terrorism in Uzbekistan. For example, by integrating AI and Big Data into the national cybersecurity system and maintaining legal balance, it is possible to increase the effectiveness of these tactics.

The use of information technologies in the fight against crimes related to terrorism has become important in the modern world. The intensification of threats in the digital environment encourages states to develop new tactics and practical approaches. The experience of countries such as Japan, South Korea, and Russia provides successful examples

in this area, and Uzbekistan has the opportunity to implement unique approaches using these practices. These experiments demonstrate the importance of a balance between technology and the human factor in the fight against terrorism.

In Japan, information technology has proven highly effective in combating terrorism. In 2020, before the Tokyo Olympics, the Japanese government paid serious attention to cybersecurity. As the Japanese scientist K. Yamada noted, "the rapid variability of threats in the digital environment requires continuous training of artificial intelligence"[21]. During this period, AI-based surveillance systems analyzed anonymous messages on the internet and identified more than 30 suspicious activities. Most of these activities were associated with radical groups, which demonstrated the technology's predictive ability.

In the practice of Japan, the use of AI provided not only a reactive, but also a proactive approach. For example, a special team from the Tokyo police used machine learning algorithms to identify radical content on internet forums and social networks. This method helped reduce the risk of cyberterrorism in Japan by 40%[22]. This experience is a successful example of cooperation between technology and law enforcement agencies.

In South Korea, tactics based on Big Data have played an important role in the fight against terrorism. In 2019, during a cyberattack operation in Seoul, the South Korean government used the Big Data Analysis method. As scholar Kim Yong-ho noted, "Big Data is capable of extracting important samples from millions of messages"[23]. In this operation, more than 50,000 messages were analyzed, and 10 potential threats were identified, five of which were related to terrorist plans.

In South Korean practice, a specially created cybersecurity agency played an important role in data collection and analysis. This agency integrated Big Data with AI to track encrypted communication tools, which allowed rapid search services to save time. As a result, the number of cyberterrorism-related crimes decreased by 25% in 2019[24]. This experiment showed the practical effectiveness of data-driven decision-making.

In Russia, information technologies were widely used in the fight against cyberterrorism. In 2018, before the FIFA World Cup, the Federal Security Service (FSB) launched a cybermonitoring system. As the Russian scientist V.V. Kozlov noted, "AI algorithms are highly effective in analyzing encrypted messages"[25]. This system detected more than 20 terrorist threats on Telegram and VKontakte platforms, which helped ensure security during the championship.

In Russian practice, special analytical tools were used to monitor social networks and decrypt encrypted messages. The system developed by the FSB was aimed at quickly identifying radical content on the Internet and preventing its spread. As a result, in 2018, the activities of 15 groups associated with cyberterrorism were suspended[26]. This experience underscores the importance of a strong link between technology and national security.

Possible approaches to the use of information technologies in the fight against terrorism-related crimes in Uzbekistan can be based on foreign experience. In 2021, a group spreading radical materials via Telegram was identified, but the full effect was not achieved due to limited technical capabilities[27]. This situation demonstrated the necessity of introducing modern technologies for Uzbekistan.

Using the experience of Japan as a first approach, it is possible to create AI-based surveillance systems in Uzbekistan. For example, a special system can be developed by teaching machine learning algorithms with Uzbek-language data to identify radical content on

social networks. This system helps operational search services quickly identify threats on the internet.

The second approach involves the use of Big Data, based on the experience of South Korea. The number of internet users in Uzbekistan has exceeded 30 million, which allows for the analysis of huge data volumes[28]. A specially created cybersecurity department can analyze messages on Telegram and other platforms to identify potential threats. This method serves to reduce the risk of cyberterrorism in Uzbekistan.

The third approach, based on the experience of Russia, is aimed at tracking encrypted means of communication. In Uzbekistan, operational-search services can detect hidden groups on platforms such as Telegram by developing special analytical tools. This method is carried out in accordance with the Law "On Operational-Investigative Activities" and maintains a legal balance[29].

References:

1. Berger, J. M., ISIS: The State of Terror, HarperCollins, 2015, p. 120.
2. FATF (Financial Action Task Force), Terrorist Financing Risk Assessment Guidance, 2019, p. 25.
3. United Nations Office on Drugs and Crime (UNODC), The Use of the Internet for Terrorist Purposes, 2012, p. 15.
Yamada, K., Cybersecurity and Terrorism in the Digital Age, Tokyo University Press, 2021, p. 45.
5. Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan, 2023 report, p. 10.
6. Criminal Code of the Republic of Uzbekistan, as amended in 2023, Articles 155 and 2442, pp. 45, 79.
7. Kim, Yong-Ho, Big Data and Counterterrorism Strategies, Seoul National University Press, 2022, p. 78.
8. FATF (Financial Action Task Force), Terrorist Financing Risk Assessment Guidance, 2019, p. 25.
9. United Nations Office on Drugs and Crime (UNODC), The Use of the Internet for Terrorist Purposes, 2012, p. 15.
Yamada, K., Cybersecurity and Terrorism in the Digital Age, Tokyo University Press, 2021, p. 45.
11. Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan, 2023 report, p. 10.
12. European Union, General Data Protection Regulation (GDPR), 2016, p. 15.
13. Kozlov, V. V., Information Technologies in Combating Cyberterrorism, Moscow: Yurayt, 2019, p. 56.
14. Kozlov, V. V., Information Technologies in Combating Cyberterrorism, Moscow: Yurayt, 2019, p. 78.
15. Sharkov, A. V., Information Technologies in Operative-Investigative Activities, Minsk: BGU, 2020, p. 45.
16. Sharkov, A. V., Information Technologies in Operative-Investigative Activities, Minsk: BGU, 2020, p. 67.

17. Yamada, K., Cybersecurity and Terrorism, Tokyo University Press, 2021, p. 34.
18. Yamada, K., Cybersecurity and Terrorism, Tokyo University Press, 2021, p. 89.
19. Kim, Yong-Ho, Big Data and Counterterrorism Strategies, Seoul National University Press, 2022, p. 102.
20. Kim, Yong-Ho, Big Data and Counterterrorism Strategies, Seoul National University Press, 2022, p. 115.
21. Yamada, K., Cybersecurity and Terrorism, Tokyo University Press, 2021, p. 34.
22. Japan National Police Agency, Cybersecurity Report 2020, 202