MAIN ENTITIES ENGAGED IN IDENTIFYING TERRORISM-RELATED CRIMES THROUGH 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.15656167

Abstract: This article focuses on the role of key actors in detecting and combating terrorism-related crimes through information technology. The article analyzes the activities of government agencies, special services, the private sector, and international organizations in this field. It examines the processes of preventing and identifying terrorist threats through the use of information technologies, particularly artificial intelligence, big data analysis, and cybersecurity tools. Special attention is also given to cooperation between entities, the legislative framework, and technological challenges.

Keywords: terrorism, information technologies, cybersecurity, artificial intelligence, crime detection, government agencies, special services, legislation.

Globalization and the rapid development of digital technologies are creating complex problems that threaten security in the modern world, particularly new forms of terrorism-related crimes. Terrorism not only poses physical threats but also seriously undermines state security through cybersecurity threats, online propaganda, and financial crimes[1]. Information technology, as a crucial tool in counter-terrorism efforts, provides effective opportunities for rapid data analysis, ensuring cybersecurity, and identifying online activities that lead to radicalization[2]. To strengthen the legal and technological foundations of counter-terrorism in the Republic of Uzbekistan, a series of reforms are being implemented, further emphasizing the importance of utilizing information technologies.

The Law of the Republic of Uzbekistan No. 167-II "On Combating Terrorism," adopted on December 15, 2000, establishes the legal framework for counter-terrorism in the country[3]. This law clearly defines the responsibilities and powers of state bodies in preventing, detecting, suppressing, and minimizing the consequences of terrorist activities. Specifically, Article 8 of the law designates the State Security Service, the National Guard, the Ministry of Internal Affairs, the State Customs Committee, the Ministry of Defense, the Ministry of Emergency Situations, the State Security Service of the President, and the Department for Combating Economic Crimes under the Prosecutor General's Office as the primary entities responsible for counter-terrorism efforts (3). The task of coordinating these bodies' activities is assigned to the State Security Service, which ensures a multi-faceted approach to countering terrorist threats through the effective use of information technologies.

The role of information technology in counter-terrorism is not limited to data collection and analysis but also encompasses critical tasks such as preventing cybersecurity threats, monitoring financial transactions, and combating online propaganda. In Uzbekistan, the 2017 amendments to the Law "On Informatization" marked a significant step in ensuring information security and combating cyber threats[4]. Furthermore, Uzbekistan's ratification of the 1999 United Nations International Convention for the Suppression of the Financing of

Terrorism in 2001 ensured compliance with international standards in detecting financial crimes through information technology[5].

As a result of the efforts of these entities, a total of 2,854 crimes (686 in 2021, 1,034 in 2022, 1,134 in 2023) related to combating terrorism and extremism were identified in our country from 2021 to 2023. Within the framework of criminal cases, 3,353 individuals (826 in 2021, 1,216 in 2022, 1,311 in 2023) were brought to criminal responsibility. - 1034, 2023. - 1134) were identified, and within the framework of criminal cases, 3,353 (2021). - 826, 2022. - 1,216, 2023.

Today, extremist and terrorist organizations are widely using the Internet to expand their ranks. As an example, we can see that 2,116 or 74% of the crimes identified in this area (476 in 2021, 833 in 2022, 807 in 2023) were committed on the Internet. It should be especially noted that citizens of the Republic of Uzbekistan who have been abroad for long periods often fall under the ideological influence of recruiters from extremist and terrorist organizations. In particular, 489 or 17% of the reported crimes (42 in 2021, 173 in 2022, 274 in 2023) were committed as a result of exposure to destructive ideas while abroad for extended periods. This indicator has been growing year by year, accounting for 6% of all crimes in 2021, 17% in 2022, and 24% in 2023. It should be especially noted that citizens of the Republic of Uzbekistan who have been abroad for a long time often fall under the ideological influence of recruiters of extremist and terrorist organizations. In particular, 489 or 17 percent of the registered crimes (2021). 42, 2022. - No. 173, 2023. - 274) as a result of long-term exposure to destructive ideas abroad.

The reasons for this include difficulties associated with social, legal, and economic adaptation, which cause alienation and psychological discomfort; disconnection from usual social ties that help form ideological immunity; separation from the oversight of relatives, close ones, the mahalla, and the public; the regulatory framework for protecting citizens who have been abroad for long periods not meeting modern requirements; and the low effectiveness of preventive measures to combat extremism and terrorism in some countries.

Of those prosecuted by these entities in the above-mentioned criminal cases, 2,013 people, or 60 percent, are young people (18-30 years old). For reference: 506 in 2021, 752 in 2022, and 755 in 2023 were young people. This figure represented 61% of those held accountable in 2021, 62% in 2022, and 58% in 2023. It is noteworthy that the main factors posing a serious threat in this regard remain the intensification of social tensions among youth, the use of the Internet for illegal purposes, extremism and terrorism, and religious organizations and sects that promote ideas rejecting secular norms and social values. This figure was 61% of those held accountable in 2021, 62% in 2022, and 58% in 2023.

As a result of operational-search measures carried out in this direction, 290 communities operating clandestinely in the republic were identified (98 in 2021, 66 in 2022, 98 in 2023). In addition, to protect the population from alien ideas and prevent offenses, a total of 32,153 awareness-raising events were conducted (11,279 in 2021, 11,210 in 2022, 9,664 in 2023), of which 19,110 (5,992 in 2021, 5,742 in 2022, 7,376 in 2023) were on topics related to terrorism and extremism. For these events, 474 video materials (203 in 2021, 227 in 2022, 44 in 2023) and 1,602 handouts (347 in 2021, 1,179 in 2022, 76 in 2023) were prepared and disseminated to the general public. - 98) communities were identified. In addition, in order to protect the population from alien ideas and prevent offenses, a total of

32,153 (2021-11 279, 2022). - 11 210, 2023. - 9,664), of which 19,110 (2021 - 5,992, 2022 - 5,742, 2023). - 7,376) on topics related to terrorism and extremism.

Although the field of cybersecurity in our country has developed significantly in recent years, there are several problems in detecting terrorism-related crimes using information technologies. Firstly, an important obstacle is the insufficient development of cybersecurity infrastructure. Modern cyber threats, particularly detecting cyberterrorism and online radicalization, require high-tech tools such as artificial intelligence, big data analysis, and blockchain, but the level of implementation and effective use of these technologies in our country does not yet fully meet the requirements[6]. For example, the lack of integration of cybersecurity systems and a unified platform for information exchange between government agencies limits the possibilities for prompt response. Secondly, the lack of qualified specialists and personnel is a serious problem. Educational programs for training highly qualified specialists in the field of cybersecurity are not yet fully developed. According to international experience, the human factor plays an important role in combating cyber threats, and without qualified personnel, it is impossible to fully utilize the technological infrastructure[7]. The lack of specialized educational institutions and certification systems for training cybersecurity specialists in our country reduces the effectiveness of activities in this area. Thirdly, the legislative framework's incomplete adaptation to cybersecurity requirements creates problems. Although Law No. 167-II "On Combating Terrorism" adopted in 2000 and the Law "On Informatization" of 2003 were important steps in ensuring cybersecurity, they are not able to fully cover modern threats such as cyberterrorism, illegal data acquisition, and online propaganda. This makes it difficult for government agencies to take effective measures against cybercrime. Fourthly, low public awareness of cybersecurity is an obstacle in the fight against online radicalization and fraud. Terrorist organizations are active in conducting propaganda via the Internet, which is successful in places where the population's digital literacy is low[8]. Although most of the population in our country uses the Internet, their knowledge of how to protect themselves from cyber threats is limited.

To address the aforementioned issues and develop the cybersecurity sector in our country, the following proposals can be put forward: It is essential to create a unified digital platform for information exchange between government agencies. This platform, based on artificial intelligence and big data analysis, would enable real-time detection and response to cyber threats. International experience shows that such platforms are effective in rapidly identifying online terrorist activities[9]. Interpol's cybersecurity platforms would be beneficial for our country. Specialized educational programs on cybersecurity, data analysis, and digital forensics should be introduced in higher education institutions. Furthermore, the qualifications of specialists can be enhanced through collaboration with international certification courses. It is advisable to establish dedicated training centers for the State Security Service and the Ministry of Internal Affairs. The Law "On Combating Terrorism" should be amended to include specific measures against crimes related to cyberterrorism, illegal data acquisition, and online propaganda. Additionally, it is recommended to develop a specific law on cybersecurity aligned with UN cybersecurity standards[10]. Public awareness campaigns on information security should be organized, and cybersecurity classes should be conducted in schools and universities. This would help protect the population from online propaganda and fraud. The European Union's public education programs on cybersecurity would be beneficial for our country[11]. Our country should foster closer cooperation with

Interpol, UN special cybersecurity groups, and other countries in information exchange and technology transfer. In accordance with the 1999 UN Convention for the Suppression of the Financing of Terrorism, it is crucial to exchange experiences in using modern technologies for tracking financial transactions[12]. Implementing these proposals will enhance the development of cybersecurity in our country and improve capabilities for effectively detecting and combating terrorism-related crimes using information technologies.

References:

1.United Nations Office on Drugs and Crime. (2019). The use of the Internet for terrorist purposes. Vienna: UNODC.

2.Weimann, G. (2015). Terrorism in Cyberspace: The Next Generation. Washington, DC: Woodrow Wilson Center Press.

3.Ўзбекистон Республикасининг "Терроризмга қарши кураш тўғрисида"ги 167-II-сон қонуни. (2000 йил 15 декабрь). lex.uz.

4.Ўзбекистон Республикасининг 2003 йил 11 декабрдаги "Ахборотлаштириш тўғрисида"ги 560-II-сон қонуни. Электрон манба: https://lex.uz/uz/docs/83472. Мурожаат вақти: 22.05.2025 й.

5.United Nations. (1999). International Convention for the Suppression of the Financing of Terrorism. Adopted by the General Assembly, 9 December 1999.

6.United Nations Office on Drugs and Crime. (2019). The use of the Internet for terrorist purposes. Электрон манба: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf. Мурожаат вақти: 22.05.2025 й.

7.Weimann, G. (2015). Terrorism in Cyberspace: The Next Generation. Электрон манба: https://www.wilsoncenter.org/publication/terrorism-cyberspace-the-next-generation. Мурожаат вақти: 22.05.2025 й.

8.Interpol. (2021). Global Cybercrime Programme: Enhancing cybersecurity through international cooperation. Электрон манба: https://www.interpol.int/en/Crimes/Cybercrime/Global-Cybercrime-Programme. Мурожаат вақти: 22.05.2025 й.

9.Interpol. (2021). Global Cybercrime Programme: Enhancing cybersecurity through international cooperation. Электрон манба: https://www.interpol.int/en/Crimes/Cybercrime/Global-Cybercrime-Programme. Мурожаат вақти: 22.05.2025 й.

10.United Nations. (2021). Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace. Электрон манба: https://www.un.org/disarmament/group-of-governmental-experts/. Мурожаат вақти: 22.05.2025 й.

11.European Union Agency for Cybersecurity (ENISA). (2020). Cybersecurity Skills Development in the EU. Электрон манба: https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu. Мурожаат вақти: 22.05.2025 й.

12.United Nations. (1999). International Convention for the Suppression of the Financing of Terrorism. Электрон манба: https://lex.uz/uz/docs/159297. Мурожаат вақти: 22.05.2025 й.