THE USE OF THE INTERNET BY TERRORIST ORGANIZATIONS

UTILIZAREA INTERNETULUI DE CĂTRE ORGANIZAȚII TERORISTE

CZU: 327.88:004.738.5 **https://doi.org/10.59295/spd2024s.32**

Cristina EJOVA,
ORCID: 0000-0003-3853-4262
e-mail: cristina.ejova@usm.md
Universitatea de Stat din Moldova

Summary. *This article examines the multifaceted ways in which terrorist organizations utilize the Internet for malicious purposes. It highlights the global expansion of the Internet and its impact on the spread of terrorist activities. Key areas of focus include propaganda, recruitment, radicalization, funding, training, planning, execution, and cyber-attacks. The study underscores how terrorists exploit the anonymity and vast reach of the Internet to disseminate extremist ideologies, attract new followers, and organize their operations. Special attention is given to the targeting of vulnerable and isolated groups, particularly minors, who are susceptible to radicalization due to psychological factors such as anger, humiliation, and isolation. The article also discusses the methodologies used in the research, including descriptive, systemic, structural-functional, and behavioral approaches, providing a comprehensive analysis of the online strategies employed by terrorist groups. The findings stress the necessity for coordinated global efforts to counteract the use of the Internet for terrorist purposes.*

Keywords: *Cyber-attacks, Internet, radicalization, recruitment, terrorist activity, terrorist financing.*

INTRODUCTION

The main characteristics of the current stage of human development are the processes of globalization and informatization, where new information and communication technologies actively penetrate all spheres of social life. The modernization of society and the development of information technologies have led to the widespread use of the Internet worldwide. More than 66% of all inhabitants of our planet use the Internet, and according to the latest data, the total number of Internet users in the world is 5.35 billion. In 2023, the Internet audience increased by 1.8%, which amounts to 97 million new users [1].

Currently, the Internet serves as a universal means of communication and information exchange for people around the world. Its undeniable advantages include the ability to reach a wide audience, the high speed of information dissemination, and its exponential nature. Additionally, the Internet provides the opportunity to conduct illegal activities anonymously. However, in the past fifteen years, there has been a trend threatening security, associated with terrorist organizations' orientation towards using Internet space. According to various studies, several thousand platforms have been created on-

line, used by terrorists and extremists to spread propaganda, recruit new members, and plan attacks.

Terrorist organizations use information and communication technologies for their malicious purposes. The main goal of terrorist organizations is to "intensify interethnic and social tensions, incite ethnic and religious hatred and enmity, propagate extremist ideology, and attract new supporters by exerting informational influence on individual, group, and public consciousness," as well as using means of destructive impact (cyber weapons) on critical information infrastructure objects. However, according to experts, "to date, there has been no recorded large-scale use of malicious software by terrorist organizations to disrupt the operation of critical information infrastructure." [2].

MATERIAL AND METHOD

In this article, a set of principles, approaches, and methods are applied to achieve the outlined goals and objectives, as well as to ensure the reliability of the obtained scientific results. We emphasize that the methodological and theoretical-scientific support of the research includes general scientific methods for understanding socio-political phenomena: the descriptive method, systemic and structural-functional approaches, and the behavioral method.

The descriptive method was widely employed to analyze events related to the use of the Internet by terrorist organizations. This method allowed for a detailed review of how terrorists use online platforms to promote their ideology and recruit vulnerable individuals.

The systemic approach is essential for understanding how terrorist organizations use the global Internet network to achieve their objectives.

The structural-functional analysis was widely used in the research process. This method allowed for a detailed examination of how terrorist organizations use the Internet to conduct their activities. By analyzing the structural components of terrorist networks and the functions they perform online, the research was able to identify the mechanisms of recruitment, propaganda, and fundraising used by terrorists on digital platforms.

The behavioral method is particularly useful in understanding how terrorists use the Internet to manipulate and radicalize individuals.

The use of logical research methods—analysis, synthesis, deduction, and induction—allows for an objective assessment of the methods terrorist organizations use to exploit the Internet.

RESULTS AND DISCUSSION

Methods by which the Internet is used for terrorist purposes

The use of the Internet for terrorist purposes represents a rapidly expanding phenomenon that requires active and coordinated countermeasures from the global community. There are no national borders for the use of the Internet in the pursuit of terrorist goals.

Additionally, the Internet is weakly regulated by state structures, allowing terrorists to operate with near impunity. While in the recent past terrorists used traditional mass media (television, newspapers, radio), with the development of modern information and communication technologies in the global space, terrorist organizations have gained access to a vast audience of users. Personal blogs, websites, forums, and personal "pages" on social networks are, in essence, mass sources of information.

Terrorists can directly engage with various audiences, who can, in turn, become active participants in an ongoing dialogue. This interaction fosters a sense of virtual community, which is often not achievable through traditional broadcast media such as radio and television [3, p. 2].

The Internet operates in almost the entire civilized world, allowing malicious actors to act on a large scale, while the costs of using this resource remain minimal.

The virtual communities created by terrorists and extremists are not tied to any specific territory. The websites and chat rooms they establish have various focuses, including religious, social, ethnic, and cultural themes, which at first glance do not arouse suspicion or concern among ordinary people. There are a great many such websites and chat rooms in the virtual space. However, regardless of the guise under which their creators operate, their goal is the same—to attract the maximum number of adherents to carry out terrorist activities [4, p.153].

Terrorist groups are taking their operations on the Internet to a qualitatively new level. For example, ISIS utilized a powerful media conglomerate within its structure, producing a wide range of multimedia content: propaganda videos, films, audio recordings of sermons, electronic versions of magazines, brochures, posters, and so on. For these purposes, the terrorist organization employed its own internet resources as well as numerous accounts on popular social networks (Facebook, YouTube, Instagram, etc.)[5].

So, the Internet has transformed terrorism in numerous ways. Activities that previously required in-person interactions, such as fundraising or training, are now carried out through websites and virtual training camps. Tools like Google Earth allow terrorists to study locations and plan potential attacks using geospatial imagery. Hacking and cyberattacks enable significant harm to be inflicted on a country's infrastructure from a computer on the other side of the world. Additionally, the Internet has become a powerful tool for terrorist propaganda and recruitment [6, p. 101].

The objectives of terrorists' activities on the Internet include: propaganda, recruitment, radicalization, and incitement to terrorism; financing; training; planning; execution; as well as computer attacks [7, p. 3]. We are going to examine the main types of terrorist activity on the Internet.

Propaganda. Modern terrorists actively and skillfully exploit the Internet's capabilities—easy access, virtually no censorship, a vast audience, anonymity, etc. Currently, they view the global network primarily as a tool for propaganda and information dissemination. Propaganda materials typically consist of multimedia communications con-

taining ideological or practical instructions, explanations, justifications, or promotion of terrorist activities. These may include virtual messages, presentations, magazines, theoretical works, audio and video files, as well as electronic games developed by terrorist organizations or their supporters [7, p. 3].

Terrorist propaganda on the Internet primarily targets the most vulnerable and isolated segments of the population. The psychological states of anger, humiliation, and isolation often create favorable conditions for the spread of terrorist propaganda, leading to radicalization and extremism. Criminals consider factors such as age, socio-economic status, religion, demographic, and ethnic characteristics. Special attention is given to minor users by terrorist and extremist websites. This group is one of the largest. The lack of critical access to information and the inability to fully analyze it create a conducive environment for messages, cartoons, or video games featuring brave terrorists and suicide bombers. In return, minor users receive rewards in the form of virtual money [8].

Recruitment. Currently, the Internet is the most effective and widespread tool for recruitment. Special attention is given to specialized websites and forums, the number of which continuously grows over time. In 1998, there were only 12 such sites, by 2005 their number had reached 4,800, and by 2013—around 10,000. The most common recruitment targets on social networks are young people with radical anti-government views, individuals with unstable mental states, those experiencing financial difficulties, and women seeking romantic relationships [9, p. 62].

Online games and the online entertainment industry have become important platforms for terrorist organizations, which use these means to promote their ideology and recruit vulnerable individuals. Computer games, as one of the main elements of mass culture, have been utilized by terrorist and extremist organizations to achieve various goals, including engaging children, spreading their ideas to a wide audience, enhancing the radicalization of supporters, and interactively constructing their ideal reality [10, p. 41]. Given the widespread popularity of computer games, extremists actively use characters, aesthetics, and plots from these games in their propaganda activities. Another striking example of the gamification of terrorist propaganda is the display of a weapon selection screen for terrorist attacks in ISIS's propaganda video "Incite the Believers." This video is designed according to computer game principles, indicating the availability of weapons for the player at the current level. Additionally, the video combines computer graphics with real footage, which, according to experts, blurs the boundaries between violence in virtual and real life [10, p. 42].

Radicalization and Incitement to Terrorism. The concept of *online radicalization* did not gain significant attention in policy and research spheres until the latter half of the 2000s. The term radicalization itself was not widely used until after the London bombings on July 7, 2005 [11, p.9]. By the early 2010s, the primary security threat had shifted towards the Islamic State. As previously mentioned, over 50,000 individuals traveled to join IS, which orchestrated and inspired hundreds of attacks. The group maintained a substantial presence on social media, with at least 46,000 IS-supporting

accounts on Twitter and thousands of foreign terrorist fighters broadcasting their lives in real time to friends and families globally. This was often facilitated by supporters who widely disseminated their content. This mobilization, coupled with IS's extensive social media reach and sophisticated propaganda, heightened concerns about the Internet's role in radicalization. UN Security Council Resolution 2178 specifically required states to address this threat, highlighting the Internet's role in inciting others to commit terrorist acts.

Another significant policy concern within the EU is the intersection between video games and radicalization. The use of games by extremist groups is not a recent development; they have been creating and appropriating games for over 20 years. However, several recent terror attacks with strong connections to gaming have heightened this concern. The former EU Counter-Terrorism Coordinator Gilles de Kerchove suggests that games and gaming platforms possess a substantial social media dimension, which can be exploited to recruit and radicalize a large, young, and vulnerable target audience [11, p.16].

Financing. An important aspect of countering the use of the Internet for terrorist purposes is combating the financing of terrorism, as terrorist organizations actively use electronic payment methods. For example, by posting electronic wallet numbers on social networks, terrorists organize schemes to collect funds for carrying out terrorist acts or extremist activities.

The rapid development and widespread use of social networks have provided terrorist organizations with new opportunities to obtain financial resources. Extremist groups actively use platforms such as Instagram, Facebook, Twitter, VKontakte, as well as mobile applications like Telegram, Viber, WhatsApp, Surespot, and VoIP, to conduct informational and propaganda work and establish contacts with potential supporters. Through these means, "sympathetic sponsors" from different parts of the world can make donations, which collectively lead to significant financial inflows for terrorists.

The emergence of crowdfunding platforms also presents a new risk for financing terrorism. These platforms can be used for illegal purposes. Often, donors on social networks and crowdfunding platforms are unaware of the ultimate destination of their donations. Individuals or organizations posing as fundraisers for legitimate humanitarian or charitable causes may actually be collecting money to provide material support to terrorist groups. Currently, extremist organizations are organizing numerous fraudulent crowdfunding campaigns to conceal their true intentions and secure financial support [9, p. 56].

Cyberattacks. The term "cyberattack" typically refers to the intentional use of computer networks to inflict damage. These attacks usually aim to disrupt the normal functioning of targets such as computer systems, servers, or critical infrastructure through hacking, sophisticated persistent threat techniques, computer viruses, malware, "flooding," or other means of unauthorized or malicious access. Cyberattacks can exhibit

characteristics of a terrorist act, particularly when their primary motivation is to instill fear in order to achieve political or social objectives [7, p. 12].

CONCLUSIONS

The use of the Internet by terrorist organizations poses a serious threat to global security. Modern information and communication technologies allow terrorists to conduct propaganda, recruitment, radicalization, training, and financing through online platforms. The Internet provides terrorists with anonymity, global reach, and low operational costs, facilitating their large-scale operations. The main objectives of terrorists on the Internet include spreading extremist ideologies, attracting new supporters, raising funds, and organizing attacks. It is important to note that terrorist propaganda particularly targets vulnerable groups, including minors, who fall victim to manipulation and radicalization. Therefore, the global community must take active and coordinated measures to counter terrorist activities in the digital space.

REFERENCES

1. Digital 2024: Global Overview Report. Available: https://www.web-canape.ru/ [Accessed: 05.07.2024]
2. Resolution A/54/49 of the UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, December 1, 1999. Available: https://documents.un.org/doc/undoc/gen/n00/324/38/img/n0032438.pdf?token=zGkHtSxV1SvTFSqtnQ&fe=true [Accessed: 05.07.2024]
3. ALY, A., MACDONALD, S., JARVIS, L., CHEN T. M. Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization. In: *Studies in Conflict and Terrorism*. 2016. nr. 40(1), p. 1-9. SSN 1057-610X (Print); ISSN 1521-0731 (Online)
4. ГАЙВОРОНСКАЯ, И., ФОМИНА, Т., АМАНЖОЛОВА, Б. Вербовка в экстремистские и террористические организации посредством сети Интернет. *Психология и право*, 2020. Том 10. № 4. С. 152–165. ISSN: 2222-5196 (online)
5. Концептуальная Записка. Противодействие использованию информационно-коммуникационных технологий (ИКТ) в террористических и экстремистских целях. Available: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Concept%20paper_30.10.2023_R.pdf [Accessed: 05.07.2014]
6. LIEBERMAN, A. Terrorism, the Internet, and Propaganda: A Deadly Combination. In: Journal of national security law & Policy 2017. Vol 9. p. 95-124
7. Использование Интернета в террористических целях. UNODC. 2013. Available: https://www.unodc.org/documents/terrorism/Publications/Use_of_

Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf [Accessed: 05.07.2014]

8. ЯНМУРЗИН, Д. ТИМЕРБАЕВ, В. Противодействие террористической пропаганде в интернете. В: *Общество, право, государственность: ретроспектива и перспектива.* 2020. №2 (2). URL: https://cyberleninka.ru/article/n/protivodeystvie-terroristicheskoy-propagande-v-internete-1 (дата обращения: 06.06.2024).
9. РАХМАНОВ, Н. Террористические организации как негосударственный субъект системы международных отношений. Диссертации на соискание ученой степени кандидата политических наук. Нижний Новгород, 2022. 185 с.
10. SUNDIEV, I., SMIRNOV, A. Gamification technologies in extremist and terrorist activities: analysis experience. In: *Scientific portal of the Russia Ministry of the Interior*. 2021. № 3 (55). P. 39–51. URL: https://cyberleninka.ru/article/n/tehnologii-geymifikatsii-v-ekstremistskoy-i-terroristicheskoy-deyatelnosti-opyt-ekspozitsii (Accessed: 06.06.2024).
11. WHITTAKER, J. Online radicalization. What we know. Luxembourg: Publications Office of the European Union, 2022. Available: https://home-affairs.ec.europa.eu/system/files/2023-11/RAN-online-radicalisation_en.pdf [Accessed: 05.07.2024]

* Articolul este elaborat în cadrul subprogramului 01.05.01 „*Securitatea națională a Republicii Moldova în contextul aderării la Uniunea Europeană: abordări juridice, politologice și sociologice*”**,** realizat de Institutul de Cercetări Juridice, Politice și Sociologice al Universității de Stat din Moldova.