

**M. Kurmanaliyev<sup>1\*</sup>** , **T. Amankul<sup>2</sup>** ,  
**R. Sarsembayev<sup>2</sup>** , **U. Tungatova<sup>2</sup>**

<sup>1</sup>Nur-Mubarak Egyptian University of Islamic culture, Almaty, Kazakhstan

<sup>2</sup>Al-Farabi Kazakh National University, Almaty, Kazakhstan

\*e-mail: maxattarazi@gmail.com

## CONTEMPORARY ASPECTS OF CYBERTERRORISM MOTIVATED BY RELIGION

The article examines the subject of religious cyberterrorism, which remains relevant in the contemporary discourse. The author underlines the possibility for terrorist organizations to form “sleeper cells” and “lone wolves” who can be deployed at any time to complete their missions. The article outlines religious terrorist organizations’ goals and propaganda methods, as well as countermeasures and counter-propaganda strategies. The relationship between their goals and propaganda tactics, information, and psychological methods of persuasion employed by propagandists is examined. The purpose of this article is to examine the information strategy of terrorist group propagandists aimed at recruiting new combatants, as well as a qualitative examination of legal, technical, and counter-propaganda methods adopted by various governments throughout the world to counteract terrorist propaganda. The author lists countermeasures and evaluates each one’s effectiveness. China is used as an example, as it is now the most effective in technological terms, despite criticism from human rights groups. As part of a counter-agitation approach, the experience of getting clergy to dispute terrorist organizations’ religious doctrine is explored. It is concluded that, notwithstanding the defeat of ISIS, the problem of opposing religious terrorist propaganda operations remains relevant today. The most essential feature of the article is the investigation of this subject within the context of Kazakhstan.

**Key words:** cyberterrorism, cyber jihad, counter-propaganda, Internet, propaganda of religious terrorist organizations.

М. Құрманалиев<sup>1\*</sup>, Т. Аманқұл<sup>2</sup>, Р. Сәрсембаев<sup>2</sup>, Ұ. Тұңғатова<sup>2</sup>

<sup>1</sup>Нұр Мұбарак Египет ислам мәдениеті университеті, Алматы, Қазақстан

<sup>2</sup>Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

\*e-mail: maxattarazi@gmail.com

### Діни мотивтенген кибертерроризмнің заманауи аспектілері

Мақала қазіргі таңда да өзекті болып отырған кибертерроризм мәселесін зерттеуге арналады. Автор террорлық ұйымдардың «ұйқыдағы ұяшықтарды» және «жалғыз қасқырларды» құрып, оларды кез-келген уақытта өз мүдделер үшін пайдалану ықтималдылығы бар екендігін атап өтеді. Мақалада діни бағыттағы террорлық ұйымдардың мақсаттары, үгіт-насихат тәсілдері, оларға тойтарыс беру және контрпропаганда шаралары келтіріледі. Автор олардың мақсаттары мен үгіт-насихат тактикасы арасындағы өзара байланыстарын, пропагандистер пайдаланатын ақпараттық және психологиялық ықпал ету әдістерін қарастырады. Мақаланың мақсаты террорлық ұйымдар пропагандистерінің өз қатарларына жаңа мүшелерді тартуға бағытталған ақпараттық стратегияларына, сонымен қатар әлем елдерінің олардың пропагандасына тойтарыс беру үшін пайдаланатын құқықтық, техникалық және контрагитациялық іс-шараларына сапалық талдау жасау. Тойтарыс беру шараларын тізбектей отырып, автор олардың әрқайсының тиімділігін талдайды. Құқық қорғаушылардың сынына қарамастан техникалық тұрғыдан қазіргі уақытта ең тиімді тәсіл болып саналатын Қытайдың мысалы келтіріледі. Контрагитация стратегиясы аясында террорлық ұйымдардың діни идеологиясын жоққа шығару мақсатында діни қызметкерлерді тарту тәжірибесі қарастырылады. Мақаланың қорытындысында ИГИЛ жеңілгеніне қарамастан террорлық ұйымдардың пропагандасына тойтарыс беру мәселесі қазіргі кезде де өзектілігін жоғалтпағаны айтылады. Мақаланың маңызды тұсы кибертерроризм мәселесі Қазақстан контекстінде қарастырылады.

**Түйін сөздер:** кибертерроризм, кибер джихад, контрпропаганда, Интернет, террорлық ұйымдардың үгіт-насихаты.

М. Курманалиев<sup>1\*</sup>, Т. Аманқұл<sup>2</sup>, Р. Сарсембаев<sup>2</sup>, У. Тунгатова<sup>2</sup>

<sup>1</sup>Египетский университет исламской культуры Нур-Мубарак, Алматы, Казахстан

<sup>2</sup>Казахский национальный университет имени аль-Фараби, Алматы, Казахстан

\*e-mail: maxattarazi@gmail.com

### Современные аспекты религиозно-мотивированного кибертерроризма

Статья посвящена исследованию проблемы кибертерроризма, который остается актуальной по сей день. Автор подчеркивает вероятность создания террористическими организациями «спящих ячеек» и «одиноких волков», которых они в любой момент могут привлечь для достижения своих задач. В статье приводятся цели, методы пропаганды террористических организаций религиозного характера, меры противостояния и контрпропаганды. Обсуждается взаимосвязь между их целями и тактикой пропаганды, информационные и психологические методы воздействия, применяемые пропагандистами. Целью статьи является рассмотрение информационной стратегии пропагандистов террористических организаций, направленной на привлечение в свои ряды новых бойцов, а также качественный анализ правовых, технических и контрагитационных мер борьбы с их пропаганды, применяемых различными странами мира. Перечисляя меры противодействия, автор анализирует эффективность каждой меры. Приводится пример Китая, который в техническом плане на данный момент является наиболее эффективным несмотря на критику правозащитников. В рамках стратегии по контрагитации обсуждается опыт привлечения священнослужителей для опровержения религиозной идеологии террористических организаций. Делается вывод о том, что проблема противостояния пропагандистской деятельности религиозных террористических организаций на сегодняшний день не потеряла своей остроты несмотря на победу над ИГИЛ. Важнейшим аспектом статьи является изучение данного вопроса в контексте Казахстана.

**Ключевые слова:** кибертерроризм, кибер джихад, контрпропаганда, Интернет, пропаганда террористических организаций.

#### Introduction

The Internet, which began to take shape in the late 20th century, has become a crucial part of nearly every aspect of our lives. Originally connecting only the small number of computers, it has since transformed into a massive global network that links billions of people. The number of users is also growing at an extraordinary pace. In today's world, the Internet has created immense opportunities for progress, ranging from easy access to information to various business endeavors.

With its arrival, obtaining information has become incredibly easier; users can find what they need with just one click. Additionally, the Internet provides numerous benefits, including extensive audience reach, privacy, swift data delivery, and the capacity to combine text, visuals, audio, and video.

These features of the Internet have drawn the interest of extremist groups, who manipulate it to further their objectives – a phenomenon known as “cyberterrorism.” Some analysts refer to this as “cyberjihad,” especially in light of recent worldwide events (Bogdan-George, 2020: 10).

Cyberterrorism, a variety of terrorism, poses a considerable threat on a global scale that remains urgent in contemporary times. Achievements in developing counter-narratives should not divert ex-

perts from the persistent issues that cyberterrorism presents. In a time characterized by rapid progress in information technology, the Internet has dissolved national borders, greatly aiding the activities of those promoting religious terrorism.

Cyberterrorism carries grave consequences that impact society, the economy, and political landscapes. From an economic perspective, large corporations frequently find themselves as primary targets, incurring substantial financial setbacks due to cyberattacks. These incidents can disrupt energy systems and impede the operations of financial institutions. Such waves of terrorism can erode a nation's credit stability and attractiveness to investors, ultimately leading to a decline in the business climate, company closures, and rising unemployment levels. Socially, it instigates turmoil within the religious sphere, inciting faith-based animosity, disturbing public order, and escalating tensions, which contribute to increased intolerance and negative perceptions of religion. For example, the emergence of ISIS ignited fervent discussions in Western society regarding the essence of Islam, intensifying anti-Muslim sentiments. In the Middle East, ISIS's propaganda not only stimulated extremism but paradoxically also provoked a rise in atheism. Politically, the consequences of cyberterrorism are noteworthy, as effective propaganda

can pave the way for the rise of religious extremists and a broader support base. Initially, the global community was largely unaware of the rise of the terrorist organization ISIS on the world stage. Capitalizing on this oversight, the group managed to seize a significant portion of Iraq, later spreading into Syria. An even more serious misstep was the world's inability to quickly identify ISIS's online propaganda efforts (Badawy, Ferraro, 2019: 21). The results were immediate. People from various nations began to flock towards this emerging terrorist group. This information spread like wildfire, deeply affecting the minds of many individuals. Enticed by ISIS's compelling narratives, a number of citizens from Kazakhstan found themselves drawn into terrorist activities. The sweeping digital propaganda campaign led by ISIS was remarkably efficient, luring individuals from all parts of the globe, including those in Kazakhstan. Many citizens, influenced by the ideologies of these extremist factions, not only aligned themselves with ISIS but also actively encouraged others in their communities to join their cause (Charlie, 2015).

Based on the information at hand, it is essential to conduct a thorough investigation into cyberterrorism, especially concerning its current and potential dangers to local religious academics. This analysis is key to devising practical approaches to counter these threats and for creating counter-narrative strategies aimed at addressing cyberterrorism.

### **Justification for the choice of topic, goal and task**

The term "cyber jihad" came into use in the early 2000s, signifying the growth of religious extremist groups navigating the worldwide digital realm. Since its introduction, these organizations have pursued a clear goal: to harness the internet for a propaganda initiative that could develop into a significant threat to security. Presently, security analysts report that these groups are focusing on creating "sleepers cells" and "lone wolves" through targeted online recruitment efforts. When these individuals are mobilized, they can be activated at strategic times and places to execute their plans (Al'bo, 2022: 18).

Kazakhstan, like other countries worldwide, is facing a new security threat: cyberterrorism. The defeat of ISIS might foster a sense of security; however, it's imperative to acknowledge that individuals connected to the group who are still free pose a risk through clandestine propaganda efforts. The online environment allows these agendas to be pursued from nearly any location across the globe. As

information technology rapidly evolves and the Internet blurs national boundaries, the tasks of terrorist propagandists have become significantly more straightforward. The global nature of cyberterrorism adds complexity to counteracting it effectively. This scenario highlights the vulnerability of nations, including Kazakhstan, to the dangers of cyber terrorism. Therefore, it is essential for Kazakh religious scholars to conduct a comprehensive examination of this issue, incorporating lessons learned from other countries' experiences in fighting cyberterrorism, in order to develop robust counter-propaganda measures.

### **Scientific research methodology**

The paper provides a conceptual analysis of the phrase "cyberterrorism." This analytical method examines the fundamental principles surrounding "cyberterrorism." The author emphasizes the distinguishing features of both "cyberterrorism" and "cyberjihad." The study concludes that both names can be used interchangeably. The research includes a content analysis of various expressions of cyberterrorism, examining the goals and propaganda methods used by terrorist organizations. Furthermore, it scrutinizes and contrasts the technical measures adopted by Western countries and China in their efforts to address cyberterrorism. Considerable focus is placed on counterstrategies and counter-propaganda initiatives, along with an assessment of their effectiveness.

### **Results and discussions**

The term "cyberterrorism" was first coined in 1980 by Barry Collin, a prominent figure at the California Security Intelligence Institute. Originally, the term referred to physical assaults on digital networks. However, as the Internet transformed into a global media outlet, its definition expanded to include the use of online platforms for spreading extremist beliefs. Despite this evolution, Kazakhstan currently lacks a clear legal framework addressing "cyberterrorism," which experts believe significantly impedes efforts to identify and thwart such activities.

The term "cyberjihad" arose during a period when the nature of terrorism increasingly acquired a religious aspect. The specific origin of this term is uncertain, but it gained visibility alongside the emergence of the ISIS group in the Middle East. Significantly, cybersecurity expert James Scott wrote a book "The Anatomy of Cyber-Jihad: Cy-

berspace is the New Great Equalizer” addressing this threat and extremist agendas in today’s interconnected world.

The theatricality of cyberterrorism increases its effectiveness: “Terrorism is theater, attacks are often carefully staged to attract the attention of the electronic media and the international press” (Jenkins 1974: 31). Each terrorist act is extensively documented, including its scope, intentions, and effects. The immense resources of the Internet have tremendously benefited religious radicals in their efforts.

It is crucial to recognize that the intention behind these terrorist groups displaying their “capabilities” online is not their only objective; they aim to achieve a range of other meaningful goals through their digital activities:

*Familiarize audience with their objectives, programs and objectives.* Terrorist organizations primarily aim, as they claim, to implement the divine laws, which leads them to target the current secular regime and its system, striving to eradicate their adversaries.

*Recruiting new supporters.* This is an ongoing priority, involving the dissemination of comprehensive information in the native language (for instance, Kazakh) about the activities, goals, supporters and enemies of the terrorist group.

*Radicalization of new members.* The radicalization process includes changing individual mindsets and promoting extremist religious ideologies through psychological manipulation.

*Raising funds.* Many foundations use the Internet to gather donations for their activities, and religious terrorist groups are no exception in this aspect. Terrorism relies heavily on continuous financial support, thus these groups actively connect with their supporters and utilize online platforms to ensure they obtain the necessary funds. Moreover, cyberattacks against banking websites are often carried out to gather sensitive information from users.

Expert analyzes in religious studies yield valuable information about the aims of religious terrorist groups, quantifying their objectives in terms of percentages.

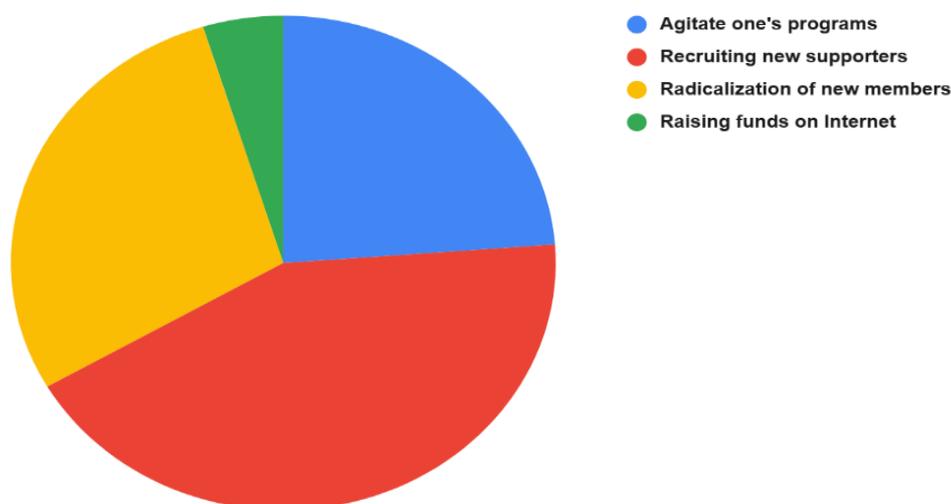


Figure 1 – Process of cyberterrorism

The propaganda methods of terrorist organizations come from the above goals. Based on religious content analysis, the following propaganda methods were identified.

*Sharia is single source of legislation.* This is the main argument in the propaganda utilized by religious extremists revolves around the assertion that a secular regime has been imposed on Muslims by the

enemies of Allah, who they identify as Western powers and their domestic allies. They contend that this imposition is the fundamental source of the problems facing the Islamic world today. According to their perspective, adopting Sharia law represents the sole solution to effectively tackle these challenges.

*Shaping an image of the enemy.* In the context of warfare, a guiding ideology is crucial, as it divides

people into two groups: “us” and “them.” This technique enables propagandists to define an adversary and inspire their supporters to take up arms against that foe. From a religious perspective, followers of these extremist factions differentiate between “believers” and “non-believers.” Importantly, the term “non-believers” encompasses not just those of other religions but also Muslims who back the existing government, collaborate with secular leaders, or subscribe to alternate interpretations of Islam (Olive, 2019: 272). For example, during the Syrian civil war, ISIS declared its intent to transform the nation into a cemetery for Shiites and specifically targeted influential Islamic figures, as seen in the 2013 assassination of Muhammad Said Ramadan al-Buti, who was killed due to his allegiance to Bashar al-Assad.

*Formation of the hero’s image.* The narrative centers on illustrating a character committed to a “holy war” who is ready to sacrifice their life for their intense goal: the establishment of Sharia law, liberating Muslims from the Western secularism, and seeking retribution against those who challenge Islam. These three elements have been emphasized by religious experts during their analysis of the content, forming the foundational message of extremist group propaganda. Their tactics go beyond these fundamental notions, employing a range of other strategies. The commonly utilized method is psychological manipulation. To enhance emotional resonance, ISIS propagandists connect with their audience through fervent, convincing, and evocative language in videos that call for individuals to join their fight against non-believers. As part of its propaganda campaign, ISIS circulated a video lecture by its leader al-Baghdadi titled “Brotherhood in Islam.” The linguistic examination of such material uncovers messages such as, “How can you, beloved brothers and sisters in faith, remain passive while your fellow believers endure suffering? On the Day of Judgment, you will face accountability for your indifference?”

The approaches used in propaganda vary depending on the target audience. While all Muslims are viewed as “targets,” the techniques employed differ greatly. Studies show that groups like al-Qaeda and ISIS tailor their communication strategies based on whether Muslims are located in predominantly Muslim nations or in countries where Muslims are a minority.

For Muslims residing in Islamic-majority countries, the propagandists associated with religious extremist groups utilized the techniques outlined in the table. No. 1.

**Table 1** – Methods of cyber terrorism

<b>For Muslims living in Muslim countries</b>	<b>For Muslims living in non-Muslim countries</b>
Criticism of the official clergy	Using a sense of belonging
Demonization of the secular regime	Demonization of everything un-Islamic, in particular the Western lifestyle
Glorifying past achievement of Muslims	Portraying non-Muslims as enemies of Muslims

Among the various critiques mentioned, the denunciation of established religious leaders is particularly significant for religious scholars. By portraying official clergy in a negative manner, extremist factions effectively position themselves as the sole guardians of what they claim to be the “authentic interpretation of faith.” For example, sociologists in Saudi Arabia noted an increase in support for Bin Laden, especially following his harsh criticisms of the well-known mufti Ibn Baz, whom he accused of constantly supporting the monarchy—views that Bin Laden argued contradicted Islamic teachings (Mahfuh, 2021: 6). From the perspective of religious studies, this strategy presents a serious danger, as it can damage the standing of official clergy among believers and simultaneously bolster the appeal of radical groups. The decline of trust or even a total loss of faith in official religious figures can have dire implications, often driving followers towards extremist organizations.

Polish Islamic expert Marcin Styshinsky conducted a thorough analysis of Al-Qaeda’s published materials and observed that the organization’s media efforts revolved around two contrasting approaches. The first strategy involved vehement criticism, allegations, and insults directed at various adversaries, including Western governments, military forces, and local authorities. Conversely, the second strategy was centered on celebrating acts of terrorism while motivating both operatives and supporters. These approaches utilized different rhetorical techniques that effectively influenced the emotions and perceptions of their audience (Styshinsky, 2017: 161-167).

Research conducted by the London Center for the Study of Extremism, known as the “Quilliam” Foundation, identifies six key themes in the propaganda of the “Islamic State”: brutality, compassion, victimhood, conflict, community, and idealism. The ferocity and aggression exhibited by ISIS militants are characterized by a celebratory tone. Through-

out various periods, ISIS has circulated disturbing videos—showcasing executions, the obliteration of ancient Palmyra, and updates from the battlefield—thereby conveying a message of dominance to its adversaries (James, 2016: 32).

The Center for the Prevention of Sectarian Derivations Related to Islam (Center de prevention contre les derivations sectaires liées à l’islam, CPDSI) asserts that Islamist groups offer “straightforward solutions to essential spiritual and existential inquiries, adeptly manipulating the concept of group identity that strongly contrasts with the broader society.” Furthermore, youthful extremists discover a “coherent value framework that eludes them in their home country” within the concept of jihad” (Roy, 2017: 55).

It is crucial to emphasize the parallels in the propaganda methods utilized by religious terrorist factions and extremist believers. A close analysis of the language these extremists employ uncovers various tactics: presenting their version of religion as the exclusive solution to all social, economic, and political issues; attacking mainstream religious authorities as pawns of governmental influence; pointing out the shortcomings of secular administrations; positioning themselves as protectors of faith while branding their opponents as threats; denouncing society for deviating from sacred teachings; inciting hostility towards anything deemed non-Islamic; and establishing a clear rift between believers and non-believers, who are labeled as agents of corruption and injustice.

These strategies do not cover all possibilities, as specialists in terrorist propaganda can create and implement more sophisticated techniques. To fulfill their objectives, they are willing to employ any methods. Therefore, to effectively combat these dangers, it is crucial for religious scholars to consistently examine the propaganda tactics utilized by religious extremists (Miron, 2023: 15).

The international community has acknowledged the threat to information security posed by ISIS and has initiated strong, multi-faceted responses. Global initiatives encompass: 1) the development of systems for exchanging effective strategies to deter foreign fighters from joining ISIS; 2) improving the sharing of intelligence related to overseas terrorists; and 3) enacting measures to locate and obstruct routes used by potential jihadists. Each nation adapts its counter-recruitment tactics according to its distinct cultural and social landscape.

Political Science Doctor A.A. Kazantsev, reflecting on European practices, identifies the following as the most effective strategies.

Developing and implementing comprehensive strategies to tackle religious extremism within the educational framework involves multiple initiatives. These include training teachers to recognize signs of youth radicalization early on, creating psychological methods to engage with affected young people, and coordinating school-based activities that address radicalism while enhancing communication skills in a diverse, multi-religious setting. Furthermore, it is essential to set up a 24-hour helpline for those facing related issues and to carry out public awareness campaigns, such as broadcasting specialized programs and public service announcements on television, along with distributing educational brochures. Moreover, it is suggested to introduce a specific course in the curriculum that focuses on critically evaluating online content (Malcolm, 2017: 101).

From a technical perspective, steps have been implemented to monitor and limit access to platforms that disseminate extremist material. Many countries have created dedicated divisions within their security services and have developed tools to monitor social media networks. The main objective is to identify and eliminate websites and accounts associated with terrorist factions. Nevertheless, specialists contend that these technical strategies often fall short, as new extremist websites tend to surface almost immediately after the removal of existing ones. The rise of social media has greatly enhanced the capabilities of terrorist groups in this regard (Cori, 2019: 18).

In this context, it is essential to highlight China’s strategy for tackling cyberterrorism. From technical standpoint, numerous specialists consider the Chinese approach to be the most efficient. To begin with, China has created its own version of the Internet, which imposes significant restrictions on foreign content, resulting in slow loading speeds or complete inaccessibility of international sites. Furthermore, the nation has implemented the “Golden Shield” initiative, designed to oversee both domestic and international web pages. This system utilizes a variety of techniques to restrict access, and although it may be technically feasible to bypass these controls, doing so can be quite difficult.

In addition, China has created a centralized information hub specifically for counter-terrorism initiatives, which is aimed at collecting data, orchestrating responses, and engaging in research. The different agencies hold the responsibility of gathering and relaying information to this counter-terrorism hub. The fundamental element of China’s Anti-Terrorism Law is its focus on the proactive

collection and application of information, which facilitates the early disruption of terrorist plots. The swift identification and immediate intervention are essential for achieving favorable results (Farhadi, 2022: 17).

Despite this, proponents of human rights in the West voice strong objections to this strategy, contending that it infringes upon the right to freely access information. It is important to recognize that these “human rights” issues create challenges in addressing cyberterrorism, given that measures such as website blocking often necessitate lengthy legal procedures. Even when such restrictions are implemented, new sites and copies tend to rapidly appear, complicating the monitoring of activities on social media platforms.

Legislative measures involve the development and implementation of a legal framework that defines the status of extremist religious groups and their affiliates. This framework encompasses strategies to curtail or eradicate illegal activities, impose penalties, and regulate the actions of state security and other governmental entities tasked with combating terrorist propaganda and recruitment efforts. However, current international legal standards are inadequate in tackling significant concerns. Important questions emerge, such as: “Should we prioritize the confidentiality of our communications or allow intelligence agencies the oversight to monitor all accounts in order to prevent terrorism?” and “Who should have the authority to regulate the Internet – the United Nations or individual states?” In our increasingly interconnected digital landscape, these dilemmas are made more complex by the global nature of the Internet. The issue of maintaining sovereignty in the digital space remains unresolved among experts. Moreover, the idea of a state-controlled Internet, similar to the model implemented in China, is impractical; for democratic countries, it indicates a withdrawal from active global participation.

In Kazakhstan, discussions indicate that initiatives for online counter-propaganda are still at an initial phase, with regulations to combat cyber terrorism just starting to be developed (Sandybaev, 2015). The legal structure aimed at tackling cyber terrorism in Kazakhstan is currently being formulated:

- Law of the Republic of Kazakhstan enacted on July 13, 1999 No. 416- I on counteraction terrorism (amended as of November 16, 2015);

- Criminal Code of the Republic of Kazakhstan “On Countering Terrorism” dated July 13, 1999 No. 416 with all amendments.

Individuals disseminating extremist ideologies on the internet may encounter both criminal and administrative repercussions. Even a simple act of sharing a post on social media can lead to scrutiny from law enforcement agencies. It is important to highlight that, as per the Criminal Code of the Republic of Kazakhstan, offenses committed through “media or information and communication networks” carry more severe penalties compared to those involving the recruitment of mercenaries, incitement to seize control, or the promotion of hatred in offline settings. This is illustrated in Articles 172 and 174 (clause 2) of the Criminal Code of the Republic of Kazakhstan, dated July 3, 2014, No. 226-V, amended on April 9, 2016. Such regulations also encompass the laws against the promotion of terrorism and extremism, calls for violent actions, and recruitment efforts.

The realm of information counter-terrorism represents a relatively new component of the established legal framework, having started to develop around 2012-2013. Notable efforts in this area were driven by terrorist events that occurred in different parts of Kazakhstan during 2011-2012. The acknowledgment of this matter by the authorities is evident through the amendment made to the Law on Countering Terrorism in 2013, which added Article 10-1. This article requires pertinent government bodies to undertake proactive measures to combat information and propaganda related to terrorism. Such initiatives include:

- explaining threats associated with terrorism;
- revealing the different methods, tactics, and approaches use to disseminate their ideologies;
- cultivating counter-terrorism mindset in society;
- bringing together government agencies responsible for fighting terrorism and community organizations to prevent such acts;
- reducing the social support network for terrorism” (Law of the Republic of Kazakhstan dated July 13, 1999 No. 416-I on countering terrorism (as amended on November 16, 2015).

Furthermore, the law mandates that government bodies work together with media outlets, private organizations, community groups, and religious leaders on efforts to tackle extremism. At the same time, from 2013 to 2014, a strong initiative was launched to implement the revised legislation. This led to the development of a governmental strategy aimed at addressing these issues, detailed in a key document—the State Program for Countering Religious Extremism and Terrorism in Kazakhstan for the years 2013 to 2017 (Makarova, 2018: 17).

This encompasses the dissemination of knowledge and educational initiatives aimed at creating media platforms to analyze radical Islamism. It contrasts this ideology with the compassionate tenets of traditional Islam while promoting humanistic ideals and encouraging harmony among different ethnic and religious groups. Additionally, it entails highlighting the violent actions of organizations like ISIS, including their recruitment of minors for warfare. In their efforts, advocates rely on the enduring values found within the Muslim community, underscoring the significance of spirituality, family bonds, and love for children (Litvinova, 2020: 33).

One significant instance of these discussions can be found in a sermon by the prominent British cleric, Abu Lait al-Maliki. In this online address, he claims that the idea of establishing a Caliphate is romanticized. He explains that the ongoing dialogue about the Caliphate arises from a yearning for earlier times, a sentiment that is often fueled among young people by radical religious figures. These extremists depict the Caliphate as an ideal society where believers live in a state akin to paradise. As a result, this narrative cultivates a sense of responsibility among young followers regarding the hardships endured by their fellow believers around the world. This feeling of obligation can lead to more extreme views. Similarly, Mohammed Nawab Osman, a professor at the Center for International Studies in Singapore, shares this perspective in his article titled "ISIS Caliphate is a Utopia." He contends that Islamic scholars need to confront the idea of a Caliphate under ISIS leadership. Bakyt Nuridinov from the muftiyat declared in an interview with Radio Azattyk that the Caliphate is only a utopia (Mohamed, 2014: 19).

Nations all across the world, including Kazakhstan, are currently working to combat cyber terrorism with their own resources. However, specialists in this field have yet to develop successful counter-propaganda methods. The exact strategy may produce variable results; it may be successful in one country but have detrimental implications in another. The technological and legal aspects of combating cyber jihad are beyond the purview of religious scholars and are instead the responsibility of recognized authorities (Molodchaja, 2011:183). The primary duty of religious scholars in combating cyber jihad is to conduct significant educational activities that emphasize the necessity of raising awareness among the country's inhabitants about the dangers and ramifications of such threats. Religious leaders can play a vital role in empowering communities and reducing the effect of radical narratives through this educational effort:

a) utopianism of the notions provided by religious terrorist groups must be carefully analyzed; notably, the idea of reconstructing the caliphate is simply a delusion offered by persons with self-serving intentions;

b) benefits and characteristics of secular regime: secular state protects individual rights and strongly opposes religious discrimination. A nation's secular character is critical for fostering interreligious peace, particularly in multi-ethnic and multi-religious societies like Kazakhstan;

c) threat of viewing information from religious terrorist organizations that can radicalize individuals and eventually change them into members of a terrorist organization;

d) risks associated with religious terrorist organizations' propaganda activities, which contain statements intended to incite interreligious hostility. This scenario largely targets Muslims' image because the faith itself may be perceived as a "source of evil," putting adherents at risk of being targets of hate (Shegaev, 2015: 5).

The development and implementation of an educational effort is an important instrument for religious leaders in fighting the influence of cyberjihad. To properly combat the major threat posed by cyberterrorism, Kazakhstan's scholars must design and implement their own propaganda operations. However, the complexity of this attempt may be beyond the capacities of local religious figures, therefore the active participation of Kazakhstan's official Muslim clergy is important.

## Conclusion

Cyberterrorism or cyberjihad, is a field of investigation that encompasses numerous subjects with multifaceted aspects that complicates its analysis.

The analysis presented in this article describes the goals and various propaganda methods used by jihadist groups. An investigation of their propaganda strategies reveals that these organizations are constantly improving and adapting their approaches, utilizing modern technologies. For example, the ISIS media unit has expanded its propaganda weapons by leveraging social media platforms, particularly Twitter. ISIS has taken advantage of different communication platforms made possible by modern Internet technology. This spike in social media activity has amplified ISIS's intellectual and operational reach, inspiring fighters worldwide to join al-Baghdadi's group (Sosnin, 2015: 22). By creating various online accounts in social networks, they effectively spread jihadist doctrines and ex-

tremist beliefs among online users, with the goal of recruiting new fighters and motivating terrorist actions. Analysts examining jihadist propaganda have identified common strategies used by al-Qaeda and ISIS. Unfortunately, ISIS has achieved great success in media warfare, equivalent to triumphs on actual battlefields. Every propaganda approach used by these terrorist media teams pursues a specific goal. For example, by criticizing official religious leaders, they portray themselves as defenders of faith, claiming to have the correct interpretation of Islam, while depicting the clergy as government pawns exploiting religion. It was highlighted that jihadists continually attempt to expand their ranks, form “sleeper cells,” and, more recently, produce “lone wolves” regardless of the techniques used. Security specialists think that lone wolves pose the most significant threat because to the limitations of tracking and identifying them at an early stage (Winter, 2018: 15).

The article examines several legal, technical, and counter-propaganda tactics for combating cyber jihad. After assessing each option, it was decided that no single strategy is uniquely successful in improving security or counter-terrorism activities. Each method has unique benefits and disadvantages. For example, technical measures can help monitor content from terrorist groups, but they fall short in counter-propaganda due to the worldwide nature of the internet (Xingxing, 2022). Blocking accounts on

social networks is inefficient as new accounts soon reemerge under other usernames. Furthermore, legal systems fail to keep up with the rapid evolution of information technology. In democratic countries, addressing concerns such as website or social media page blocking requires a judicial decision, which can take weeks or even months. Furthermore, proposed technical and legal solutions frequently attract substantial resistance from human rights advocates, who say that such activities violate the right to freely access information. Technically, China displays a strict approach to cyber terrorism by creating a controlled internet and rigorously monitoring foreign materials for extremist content. Ultimately, governments dealing with cyber terrorism have a difficult decision between human rights protections and public safety. This dilemma has also surfaced as a contentious subject among Kazakhstani religious experts, stressing the need for additional investigation into this topic.

### Acknowledgment

This research was funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP22685041. Exploring the social-psychological aspects of religious education in secondary and special secondary educational institutions regarding the promotion of tolerance).

### References

- Badawy A., Ferraro, E. (2019) The rise of Jihadist propaganda on social networks. *Journal of Computational Social Science*, vol. 4, no 3. – 21-22.
- Farhadi A. (2022) Countering Violent Extremism in Central Asia and South Asia. *Journal The Great Power Competition*.
- Al’bo T. (2022) Propagandistskaja dejatel’nost ‘ IGIL i method bor’by s nej [Propaganda activities of ISIS and methods of combating it]. *Vestnik Volzhsky university imeni V.N. Tatishheva*, vol. 2, no. 2.
- Bogdan-George R. (2020) The “Electronic Jihad” How Social Media are Used for Disseminating Terrorist Propaganda. *Medea Egysület*. – 9-10
- Cori E.D., Robinson D., Jovan J.B., Austin G.B. (2019) Call of Duty: Jihad—How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. *Perspectives on Terrorism*, vol.13, no. 3. – 17–31.
- James S., Drew S. (2016) The Anatomy of Cyber-Jihad. Cyberspace Is the New Great Equalizer. *Washington DC: Institute for Critical Infrastructure Technology*. – 31–33.
- Litvinova T.N. (2020) Evropejskaja i rossijskaja politiki antivodejstvija cyberterrorism (na primere bor’by s “kiber-dzhihadom”) [European-Russian policy against cyberterrorism (based on the fight against cyberterrorism)]. *Nacional’naja bezopasnost*, no. 3. – 32 – 47.
- Mahfuh B. H., Muhammad S. (2021) Religious extremism: Challenging extremist and jihadist propaganda. *Annual threat assessment*. – 5-6.
- Makarova E. J. (2017, June 15) Profilaktika i bor’ba s cyberterrorizmom v Kitae [Prevention and Combating of Cyber Terrorism in China]. *Sbornik Nauchnoj prakticheskoy konf. Belgorod*. – 16-18.
- Malcolm N., Chris S. (2017) *Hacking ISIS: How to Destroy the Cyber Jihad*. Skyhorse Publishing, New York. – 174.
- Miron L. (2023) Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad. *Journal Terrorism and Political Violence*, Vol, 23. – 189-207.
- Mohamed N. (2014) ISIS’s caliphate utopia. *RSIS Commentaries*, Singapore: Nanyang Technological University.

Molodchaja E.N. (2011) Politika antivodejstvija cyberterrorizmu v sovremennoj Rossii: politologicheskij aspekt [Anti-cyberterrorism policy in modern Russia: political science aspect]. *Dis. ... kand. Polit. Nauk*. Moscow. – 188.

Olive R. (2019) Francuzskie radikalny – kto oni? [French radicals – who are they?]. *Religii i radikalizm v postsekuljarnom mire*. – 263-265.

Roy, Olivier (2017) *Jihad and Death. Global Appeal of Islamic State*. Hurst Publishers. – 36.

Sandybaev A. (2015, June 16). Chto oznachaet tysjacha zaverbovannyh iz Kazakhstan v IG? [What does it mean that there were a thousand recruits from Kazakhstan to ISIS?]. *Polucheno iz Radio Azattyk*. <http://rus.azattyq.org/content/terrorizmigil-kazakhstan/27075180.html>

Shegaev I.S. (2016) Sovremennyyj terroristicheskij rekruting: systemy i principy [Modern Terrorist Recruitment: Systems and Principles]. *Vestnik Moscow state government oblastnogo universiteta*, no. 1. – 1-12.

Sosnin V.A. (2015) Sovremennyyj terrorism i problema verbovki ljudej v terroristicheskie seti: psihologicheskie aspekty [Modern terrorist and the problem of recruiting people into terrorist networks: psychological aspects]. *Prikladnaja juridicheskaja psihologija*, no. 4. – 20–28.

Styshinskij M. (2016) Dzhihadistskaja propaganda v internete i social'nyh media [Jihadist propaganda on the Internet and social media]. *Politicheskaja lingvistika*, no. 2. – 161–167.

Winter Ch. (2015) *The Virtual 'Caliphate': Understanding the Islamic State's Propaganda Strategy*. Quilliam. – 52.

Xingxing W. (2022) A critical evaluation of China's legal responses to cyberterrorism. *Computer Law and Security Review Journal*, vol. 47.

#### **Information about authors:**

*Kurmanaliyev Maksat (corresponding author) – PhD student of Nur-Mubarak Egyptian University of Islamic Culture Nur-Mubarak (Almaty, Kazakhstan, e-mail: maxattarazi@gmail.com).*

*Amankul Temur Oralbaiuly – PhD, senior lecturer of the Department of Religious Studies and Cultural Studies, Al-Farabi Kazakh National University (Almaty, Kazakhstan, e-mail: amankul\_2007temur@mail.ru).*

*Sarsembayev Ruslan Meirzhabuly – PhD, senior lecturer of the Department of Religious Studies and Cultural Studies, Al-Farabi Kazakh National University (Almaty, Kazakhstan, e-mail: Rus\_tk007@mail.ru).*

*Tungatova Ulzhan Askarbaikyzy – PhD, senior lecturer of the Department of Religious Studies and Cultural Studies, Al-Farabi Kazakh National University (Almaty, Kazakhstan, e-mail: tua20@mail.ru).*

#### **Авторлар туралы мәлімет:**

*Құрманалиев Мақсат (корреспондент автор) – Нұр Мұбарак Египет ислам мәдениеті университетінің PhD докторанты (Алматы, Қазақстан, e-mail: maxattarazi@gmail.com).*

*Аманқұл Темур Оралбайұлы – PhD, әл-Фараби атындағы Қазақ ұлттық университеті дінтану және мәдениеттану кафедрасының аға оқытушысы (Алматы, Қазақстан, e-mail: amankul\_2007temur@mail.ru).*

*Сәрсембаев Руслан Мейіржанұлы – PhD, әл-Фараби атындағы Қазақ ұлттық университеті дінтану және мәдениеттану кафедрасының аға оқытушысы (Алматы, Қазақстан, e-mail: Rus\_tk007@mail.ru).*

*Түнгатова Ұлжан Асқарбайқызы – PhD, әл-Фараби атындағы Қазақ ұлттық университеті дінтану және мәдениеттану кафедрасының аға оқытушысы (Алматы, Қазақстан, e-mail: tua20@mail.ru).*

#### **Сведения об авторах:**

*Құрманалиев Мақсат (автор-корреспондент) – PhD докторант Египетского университета исламской культуры Нур-Мубарак (Алматы, Казахстан, e-mail: maxattarazi@gmail.com).*

*Аманқұл Темур Оралбайұлы – PhD, старший преподаватель кафедры религиоведения и культурологии Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: amankul\_2007temur@mail.ru).*

*Сәрсембаев Руслан Меиржанович – PhD, старший преподаватель кафедры религиоведения и культурологии Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: Rus\_tk007@mail.ru).*

*Түнгатова Ұлжан Асқарбаевна – PhD, старший преподаватель кафедры религиоведения и культурологии Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: tua20@mail.ru).*

*Received: February 27, 2024.*

*Accepted: September 9, 2024.*