IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Analysis of modern types of cyberterrorism and methods for countering them

Kakimzhan Bishmanov
Al-Farabi Kazakh National University

Zarina Muratzhan
M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan

Zhanat Dilbarkhanova
M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan

Viktoriya Lyutsik
Turan University

Date of submission: May 2024
Accepted in: July 2024
Published in: October 2024

Abstract

In light of the accelerated digital development, the heightened reliance on information technologies, and, at the same time, the growing threat of cyberterrorism, this study aims to develop efficient strategies to counter contemporary cyber threats. Methods such as experimentation, comparison, analysis, and synthesis were employed to achieve this purpose. The study's main results encompass a broad overview and analysis of modern forms of cyberterrorism and their key characteristics. As part of the study, a plan to combat cyberterrorism is implemented, incorporating diverse strategies and methods for preventing cyber threats. Python code is used to track network traffic, analyse data transmission, and block nodes causing harm, aiding in detecting and preventing potential cyberattacks. A structural scheme is developed to systematize the process of countering cyberattacks, containing a detailed action plan. The scheme starts with detecting potential attacks and ends with analysing the measures' effectiveness and planning for future steps. In addition, real-world examples of global cyberattacks are provided, and other studies on this issue are examined. The practical value of this study lies in providing concrete recommendations and ways to enhance cybersecurity at both governmental and corporate levels.

Keywords

cyber threats; cybersecurity; information protection; information technology

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Análisis de tipos modernos de ciberterrorismo y métodos para contrarrestarlos

Resumen

A la luz del desarrollo digital acelerado, la creciente dependencia de las tecnologías de la información y, al mismo tiempo, la creciente amenaza del ciberterrorismo, este estudio tiene como objetivo desarrollar estrategias eficientes para contrarrestar las ciberamenazas contemporáneas. Se emplearon métodos tales como la experimentación, la comparación, el análisis y la síntesis para lograr este propósito. Los resultados principales del estudio abarcan una amplia descripción general y análisis de las formas modernas de ciberterrorismo y sus características clave. Como parte del estudio, se implementa un plan para combatir el ciberterrorismo, incorporando diversas estrategias y métodos para prevenir las amenazas cibernéticas. Se usa código Python para rastrear el tráfico de red, analizar la transmisión de datos y bloquear nodos que causen daños, lo que ayuda a detectar y prevenir posibles ciberataques. Se desarrolla un esquema estructural para sistematizar el proceso de contrarrestar los ciberataques que contiene un plan de acción detallado. El plan comienza con la detección de posibles ataques y termina con el análisis de la efectividad de las medidas y la planificación de los pasos futuros. Además, se proporcionan ejemplos reales de ciberataques globales y se examinan otros estudios sobre este tema. El valor práctico de este estudio reside en proporcionar recomendaciones concretas y formas de mejorar la ciberseguridad tanto a nivel gubernamental como corporativo.

Palabras clave

ciberamenazas; ciberseguridad; protección de la información; tecnología de la información

1. Introduction

The relevance of information security issues is growing in today's information society, as digital technologies are integral to many aspects of life. Cyberterrorism is one of the most significant risks nowadays, which necessitates ongoing research. It is vital to continuously update the techniques for safeguarding data and information systems due to the rapid advancement of digital technology and the rise of cyberattacks. The issue of the study is that, as cyberattacks become more sophisticated, strategies for countering modern digital threats must be developed. Current data and information security techniques frequently prove to be insufficiently successful. Investigating and identifying critical weaknesses in current cybersecurity techniques is essential, as is developing new tactics to fortify defences against cyberterrorism.

For a more thorough analysis of this issue, it is advisable to consider other studies that include methods for combating cyberterrorism. For example, Alimseitova and Beketova (2022) analysed network attacks and methods for their detection. They explored methods for detecting and classifying patterns in Internet systems using neural network models. The analysis of the conducted research allowed them to identify the effectiveness of some classical types of neural networks for solving this problem; however, they also identified some limitations and issues in the operation of these models.

Researchers Akhmetov and Aidarkul (2023) emphasised that cyber threats are becoming increasingly acute for many private companies and government organisations worldwide due to the rapid development of digital technologies. Difficulties ensuring cybersecurity are significantly increasing due to the constant threat of cyberattacks on electronic systems. Researchers worldwide are exploring various methods for preventing cyber threats and their consequences, noting the need to develop security standards and exploring the latest trends and innovations in cybersecurity. Like the previous authors, Ospanova *et al*. (2021) and Movchan *et al*. (2023) analysed the areas of cybersecurity, information security, and artificial intelligence. They developed useful mobile applications based on Raspberry Pi microcomputers to protect corporate and home networks. The results of their study demonstrated significant potential for using such technologies in cybersecurity, including the development of syntactic and semantic analysers and linguistic processors.

In turn, Amirova and Tohmetov (2022) explored the necessity of detecting and preventing cyber threats in the Industrial Internet of Things (IIoT) context. The unique features of IIoT increase the complexity of protection against cyberattacks.

These issues become more significant due to the growing demand for these technologies. The study by Kalmurzaev *et al*. (2021) conducted a comparative legal study on national legislation combating religious extremism compared to the bill of some foreign countries. The researchers analysed the theoretical foundations of the comparative legal method and research methods in legal science in the context of terrorism, including methods of combating it.

The listed studies mainly focused on analysing existing threats and types of cyberattacks, as well as identifying vulnerabilities in information security systems. However, they omitted a thorough examination of effective strategies for mitigating cyberterrorist threats, establishing security standards, and scrutinising the most recent developments in cybersecurity. Furthermore, many did not pay sufficient attention to analysing strategies and technologies for preventing cyber threats, leaving gaps in understanding the mechanisms for protecting against cyberattacks. As a result, there is a need for further research to delve into these aspects to develop more effective methods for combating cyberterrorism.

Therefore, the research aims to develop practical strategies for countering contemporary cyber threats. To achieve the overall goal of protecting against cyberattacks, the following tasks were identified: analysing effective countermeasures for cyberterrorist threats, thoroughly examining technologies and strategies for preventing cyber threats to determine their benefits and drawbacks, and formulating recommendations for creating and implementing trustworthy defences against cyberattacks at different levels based on research findings.

1. Materials and methods

The study used various approaches, including comparative and experimental methods, to analyse and effectively combat cyberterrorism. Using an experimental approach, a Python code was created to analyse network traffic and data transmission and automatically prevent suspicious activity. This experiment was essential to assessing the program's effectiveness and confirming that it could recognise and thwart possible cyberattacks. Researchers were able to simplify the development process and guarantee the dependability of the defensive systems against cyber threats by using the Replit development environment, which allowed them to program comfortably and test the developed code immediately. This strategy offered useful real-time performance data, enabling modifications and enhancements to boost the program's efficacy in thwarting cyberattacks. Thus, the experimental approach proved essential to the cybersecurity software development process, offering valuable insights and guaranteeing a strong defence against cyberattacks.

The comparative approach was employed in addition to the experimental method to produce an extensive table that contrasted the traits of different forms of cyberterrorism. This technique organised data regarding various cyberattack kinds, emphasising key characteristics for further examination. Additionally, it made it easier to compare multiple tactics and approaches to address cyber threats and determine the benefits and drawbacks of each in relation to the fight against cyberterrorism. The best methods for fending off cyber threats were identified through this comparative research, which served as the foundation for an all-encompassing plan to prevent cyberterrorism. Given the complexity of contemporary threats and challenges in the field of cybersecurity, the comparative method allowed for the development of more focused and tailored methods for cyber threat mitigation by identifying the critical aspects that determine the effectiveness of combating cyberterrorism. This approach established the framework for developing an elaborate plan that combined the most effective and suitable methods to ensure consistent network and information system protection.

Analysis and synthesis techniques were essential for comprehending complex problems and creating workable solutions. Researchers determined key trends, contemporary issues, and scientific advancements in cybersecurity by examining the body of literature on cyberterrorism. At this point, a comprehensive analysis of previous research in the area was conducted to understand better how it contributed to the fight against cyberterrorism. The information gathered from these analyses was then compiled and organised using the synthesis approach to create a more comprehensive picture of the issue. These techniques made it possible to identify essential components of cyberterrorism, uncover knowledge gaps, and develop fresh strategies for researching and countering this danger. Synthesis and analysis methods made it possible to move from looking at discrete parts of cyberterrorism to doing a thorough analysis and developing integrated measures to address this issue. As a result, these techniques served as the cornerstone for creating plans to combat cyberterrorism and for creating fresh concepts and suggestions in this field.

2. Results

2.1. Cyberterrorism landscape: overview and comparative analysis

Cyberterrorism involves the use of modern technologies for terrorist purposes. This may include actions such as attacks on information systems, hacking, data theft, or disruption of online services. Cyberterrorism's goals include causing economic and physical damage, influencing public opinion, creating panic or fear, and achieving political aims, including coercing governments or organisations into specific actions. They may also engage in cyber extortion, threatening to carry out attacks if certain demands are unmet. The diversity of cyberterrorism manifests in its various areas (Table 1).

Table 1. A comparative table of different types of cyberterrorism

Types of cyberterrorism	*Characteristics of the attacks*
Cyberterrorism against government facilities	Attacks on government websites
	Cyber espionage
	Disruption of critical infrastructure
Cyberterrorism against financial systems	Attacks on banks and financial institutions
	Cyber espionage
	Financing of terrorism
Cyberterrorism against individuals	Cybercrimes
	Spreading disinformation
	Cyberbullying
Cyberterrorism motivated by ideology	Attacks on Islamist extremist websites
	Attacks on the websites of anti-fascist activists
Cyberterrorism against social groups	Attacks on the websites of sexual minority communities
	Attacks on the websites of feminist organisations

Source: own creation

Cyber espionage involves infiltrating computer networks to steal confidential information. Attacks on the power grid and transportation systems disrupt critical infrastructure. Attacks on financial systems include theft of money, DDoS attacks, and fraudulent transwactions. Terrorism financing can be facilitated through online payments and cryptocurrencies. Attacks on private individuals may involve theft of personal data, fraud, and extortion. Disinformation can be spread to sow panic or chaos, and cyberbullying can be directed at harassment in the online environment. Ideologically motivated cyber-attacks may target websites of Islamist extremists or anti-fascist activists (Tymoshenko, 2022). Cyberterrorism targeting social groups includes attacks on websites of sexual minority communities and feminist organisations.

It is worth providing examples of cyberterrorist acts to understand this issue better. For instance, in February 2024, confidential data from the Chinese company iSoon, a contractor for the Ministry of Public Security of China, was leaked on the GitHub platform (Kim, 2024). This company is linked to a structure controlled by China's cyber espionage group known as APT41. As a result of the leak, critical infrastructure objects of several countries, including Kazakhstan, became accessible. In addition, data on telecommunications operators and subscriber information were disclosed. The attacks lasted for over two years, allowing hackers to gain full access to telecommunication critical infrastructure, control over event logs, and access to user data. This incident revealed systemic flaws in information security.

A ransomware assault occurred on 7 May 2021, affecting Colonial Pipeline, which provides petroleum to over half of the East Coast (Snager *et al*., 2021). The assault, ascribed to the ransomware organisation DarkSide, resulted in the pipeline's operations being shut down, which caused severe gasoline shortages and panic purchasing. To get back into the attackers' systems, Colonial Pipeline paid them a $4.4 million ransom; nevertheless, the U.S. Department of Justice eventually recovered some of the payment. This incident brought awareness to the weaknesses in key infrastructure and the increasing risk of ransomware attacks on vital services.

In December 2023, a massive cyberattack named UAC-0050 was discovered, utilising the malicious software (malware) RemcosRAT/MeduzaStealer and targeting Ukraine and Poland (Massive cyberattack UAC-0050..., 2023). Data about the attack was published on the website of the Computer Emergency Response Team of Ukraine. As part of this attack, phishing emails with malicious attachments were sent using legitimate but compromised accounts, including the domain gov.ua. If recipients opened the attached archives, their computers could become infected with the RemcosRAT or MeduzaStealer malware. Possible victims included government agencies in Ukraine and Poland. Measures were taken to detect and prevent the threat, and it was recommended to filter emails with protected passwords on mail servers (Borko & Vilks, 2023). These are just some examples highlighting the scale and diversity of threats posed by cyberterrorism.

2.2. Implementation of the cyberterrorism counteraction plan

Cyberterrorism, as a modern phenomenon, requires the development of effective counter-strategies to ensure the security of information systems and protection against potential threats (Vilks *et al*., 2022). To achieve this goal, a strategy to combat digital terrorism should be developed, including a range of methods and activities to prevent attacks, protect data, and ensure the stable operation of information infrastructure.

Methods to counter cyberterrorism may include strengthening the protection of information systems, training personnel, monitoring and analysing threats, creating data backups, international cooperation, and developing and implementing modern encryption technologies. In addition, it is important to consider active updating and maintenance of software, implementing multi-level authentication systems, creating "whitelists" and "blacklists" networks, conducting simulations and training exercises for responding to cyberattacks, applying analytical systems and artificial intelligence, creating and supporting international legal frameworks. In other words, an important aspect of combating cyberterrorism is ensuring reliable protection of information systems from external attacks. This includes installing and regularly updating antivirus programs, firewalls, intrusion detection systems, and other security measures.

Often, the weakest link in a security system is the employees, who can fall victim to social engineering or errors in the safe use of information resources (Kanybekova *et al*., 2023). Conducting regular training and education sessions for employees on the basics of cybersecurity helps reduce the risk of successful cyberattacks. Continuous monitoring of the information environment allows for the timely detection of suspicious activity and potential threats. The analysis of attack data helps identify the characteristics and methods used by cyberterrorists, aiding in further improvement of the counter-strategy. In the event of a successful cyberattack, it is important to have the ability to restore data quickly. Regular creation and storage of backups minimise losses during cyberattacks and reduce recovery time after an incident. Cyberterrorism knows no borders, so cooperation and coordination between states and international organisations are important to combating this phenomenon. Information exchange on threats, joint exercises, and developing international security standards help effectively counter cyberterrorism (Arstanbekov *et al*., 2024; Metelskyi & Kravchuk, 2023). Features of cybercrime and its prevalence in Ukraine.

Using strong encryption algorithms to protect confidential information helps prevent unauthorised access to data even in the event of successful infiltration by attackers. Regular updating of operating systems and application software helps eliminate vulnerabilities known to attackers and prevents the exploitation of these vulnerabilities for cyberattacks. Using multi-factor authentication methods (such as passwords, one-time codes, and biometric data) enhances the security of user accounts and reduces the risk of compromise of logins and passwords. Developing and maintaining databases of known trusted and suspicious Internet Protocol (IP) addresses, domain names, and network protocols allows for effective traffic filtering and blocking potentially dangerous connections. Organising

regular training scenarios and incident simulations allows staff to gain experience and skills in quickly responding to cyberattacks and optimising response and recovery procedures after incidents. Using data analytics and artificial intelligence tools to monitor and detect unusual or suspicious activity helps quickly identify potential threats and respond to them before damage is done. Developing international cooperation in cybersecurity and creating unified legal standards and mechanisms for responding to cyberattacks allow for effective global counteraction against cyberterrorism (Shopina *et al*., 2020; Sopilko & Rapatska, 2023).

Thus, implementing the counterterrorism plan is based on a comprehensive approach, which includes technical and organisational measures to prevent and minimise the consequences of cyberattacks.

2.3. Software implementation of cybersecurity strategies

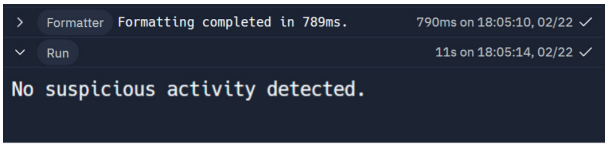
It is worth developing a specific program to visualise this concept. For example, Python code that monitors network traffic analyses data transmission and automatically blocks suspicious nodes, allowing for the detection and prevention of potential cyberattacks.

```
import time
import random

class NetworkMonitor:

 def __init__(self):
 self.network_traffic = {} # Dictionary for storing network traffic
 self.suspicious_nodes = set() # Set for suspicious nodes
 self.blocked_nodes = set() # Set for blocked nodes

 def capture_traffic(self, packet, source_ip):
 if source_ip not in self.network_traffic:
 self.network_traffic[source_ip] = [
 ] # Creation of a list for each IP address
 self.network_traffic[source_ip].append(
 packet) # Adding a packet to the list for a given IP address

 def analyze_traffic(self):
 for ip, packets in self.network_traffic.items():
 for packet in packets:
 if «malicious» in packet.lower(
 ): # Checking for suspicious nodes
 self.suspicious_nodes.add(
 ip
 ) # Adding an IP address to a lot of suspicious nodes

 def block_suspicious_nodes(self):
 if self.suspicious_nodes: # Checking for suspicious nodes
 print("Blocking suspicious nodes:") # Blocking message output
 for ip in self.suspicious_nodes:
 print(f»Blocked node with IP address: {ip}»
 ) # Output of blocked nodes
 self.blocked_nodes.add(
 ip
 ) # Adding a blocked node to the corresponding set
 else:
 print(«No suspicious activity detected.»
 ) # Display of a message about the absence of suspicious activity

 def clear_traffic(self):
  self.network_traffic.clear() # Clearing network traffic data
 print(«Cleared network traffic data.»
 ) # Output of a data cleanup message

 def display_blocked_nodes(self):
 if self.blocked_nodes: # Checking for blocked nodes
 print("Blocked nodes:") # Output of a message about blocked nodes
 for ip in self.blocked_nodes:
 print(f»Blocked node with IP address: {ip}»
 ) # Output of blocked nodes
 else:
 print(«No nodes are currently blocked.»
  ) # Displaying a message about the absence of blocked nodes


# Usage example
monitor = NetworkMonitor()

for i in range(1000):
 packet = f»Packet {i}»
 source_ip = f»192.168.1.{random.randint(1, 10)}" # Generating a random IP address
  monitor.capture_traffic(packet, source_ip) # Capturing network traffic
 time.sleep(0.01) # Delay to simulate traffic transmission

monitor.analyze_traffic(
) # Network traffic analysis for suspicious packets
monitor.block_suspicious_nodes() # Blocking suspicious nodes
monitor.clear_traffic() # Clearing network traffic data
monitor.display_blocked_nodes() # Displaying blocked nodes
```

This program operates by capturing and analysing network traffic passing through the network interface. It checks each network packet for suspicious signs, such as abnor-

mal data volume, strange requests, or unusual ports. If suspicious activity is detected, the program automatically blocks access from the corresponding node to the network to prevent a potential cyberattack. In addition, it records information about blocked nodes, enabling the analysis of potential threats and the implementation of appropriate measures to prevent them. The program output includes a log of all blocked nodes, containing detailed information about the type of attack, detection time, and additional details such as IP address and port. The program issues a warning or notification to the system administrator about detected cyber threats to take additional security measures for network security (Figure 1).

Figure 1. Program output



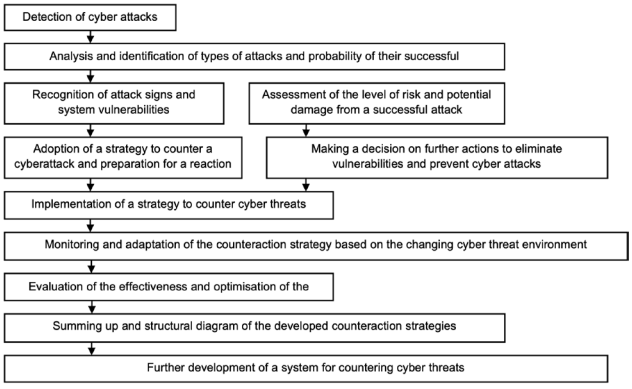
Source: own creation

In essence, this program is a comprehensive tool for detecting and preventing cyberterrorism threats. It effectively protects information systems from potential attacks and minimises the risk of confidential data leakage or network disruption.

2.4. Summary

To systematise the process of countering cyber threats, a structural scheme representing a detailed action plan for combating the specified threats can be considered (Figure 2).

Figure 2. A block diagram of countering cyber threats



Source: own creation

This block diagram includes a sequence of stages, starting from detecting potential attacks and ending with analysing the effectiveness of measures taken and planning further actions. It helps systematise the process of countering cyber threats, optimise resources, ensure a comprehensive approach, and create a foundation for development (Akylbayeva *et al*., 2014).

In conclusion, certain recommendations should be highlighted. It is worth encouraging continuous updating and improvement of strategies to counter cyberterrorism, considering emerging threats and the latest technologies in cybersecurity. Moreover, regular training and drills for staff on cybersecurity measures are necessary for effective response to threats and minimising potential consequences. Continuing and deepening international cooperation in cybersecurity is essential for information exchange, developing joint strategies, and coordinating actions. Attention should be paid to increasing investments in developing and implementing modern technologies and methods to protect information systems from cyber threats, such as artificial intelligence, machine learning, and quantum cryptography. Furthermore, it is crucial to develop and refine legal regulations in the field of cybersecurity to establish accountability for cyberattacks and protect the rights of consumers and organisations.

In general, it is worth noting that successful counteraction to cyberterrorism requires an integrated approach, which includes technical, organisational, and legal measures. Only through joint efforts of states, international organisations, the private sector, and the public can security in the digital environment be ensured and information resources protected from cyber threats.

3. Discussion

Cyberterrorism is a serious and dynamic threat in the current digital era that calls for careful consideration and well-thought-out countermeasures. Numerous research examining the complexities and problems involved in combating cyberterrorism highlight how urgent it is to confront this studies.

For example, Montasari (2024) analysed machine learning methods underlying counterterrorism efforts, focusing on cyberterrorism. He explored the complexities of applying

artificial intelligence and machine learning in this field, including ethical and legal issues. The study addresses security aspects, transparency, unwanted consequences, and proposes strategies to address identified problems. The study significantly contributes to understanding the challenges of applying machine learning in combating cyberterrorism and identifies ways to ensure security and protect fundamental human rights. In contrast, the current study focuses on developing strategies to counter contemporary cyber threats. Both studies discuss the challenges of applying specific technologies in this field and the complexities of applying certain technologies in this field. However, the second study also examines safety aspects and offers practical recommendations, while Montasari's study focuses on identifying complexities and providing common problem-solving strategies.

Siddha and Benarrivo (2023) emphasised that information and communication technologies substantially impact various aspects of life in Indonesia. They conducted an analysis examining the state's response to cyberterrorism and underscored the importance of internal and external aspects in decision-making. Indonesia seeks to enhance its capabilities through international cooperation, but challenges such as organisational culture and institutional barriers remain, requiring attention. Thus, the researchers of this study focused on developing methods to prevent cyber threats, while the study by Siddha and Benarrivo is centred on the state's response to cyberterrorism and the importance of internal and external aspects in countering this phenomenon. Both papers emphasise the need to improve state capabilities through international cooperation, but the results, mentioned above, delve deeper into specific ways to counter cyber threats.

The study by Salih and Al Alazzam (2023) examined the use of modern information technologies, highlighting society's vulnerability to cyber-attacks. Many international organisations are grappling with this threat, including universities that train cybersecurity specialists. The study explores the role of legal colleges in combating cyberterrorism and identifies the necessary competencies for future cybersecurity professionals. It is concluded that educational institutions play a substantial role in countering cyber threats. Thus, both studies draw attention to the role of modern technologies and society's vulnerability to cyber threats. However, the current study focuses on developing strategies to counter cyberterrorism, while the research by Salih and Al Alazzam emphasises the role of colleges in this process. In other words, the latter study specifically addresses education-related aspects and the competencies of future cybersecurity professionals.

Cantika and Umniyah (2023) discussed the strategies employed by Australia to counter cyberterrorism. Many countries recognise terrorist groups as a global threat. Globalisation has contributed to the emergence of cyberterrorism, which terrorist groups use for propaganda, recruitment, and attack planning. The Australian government has taken various measures to counter this threat, including legislative initiatives and the establishment of cybersecurity centres. As in the current study, the mentioned study notes the rise of cyberterrorism and the importance of global efforts to combat this threat. However, unlike this paper, which focuses on developing methods to counter cyberterrorism, the study by Cantika and Umniyah is more oriented towards specific measures the Australian government takes, such as legislative initiatives and establishing cybersecurity centres.

Like other authors, Butler and Montasari (2023) explored the impact of the Internet on cyberterrorism processes and attempts to counter them. They also examined physical terrorism, ways in which terrorist organisations use the Internet, and its application in attack planning and execution. The paper discussed the role of artificial intelligence in cybersecurity and its potential application for national security protection, including potential issues and the influence of the Internet on terrorist attack processes and countermeasures. Both studies address the impact of the Internet on cyberterrorism processes, methods of countering them, and the role of artificial intelligence. Nevertheless, the study by Butler and Montasari also developed methods to combat classical terrorism, while the latter study on cyberterrorism focused only on creating methods to counter information threats.

Leštanin and Nikac (2022) focused on the fact that computers and the Internet play an important role in modern society. However, their use poses problems related to cybercrime. The researchers discuss the efforts of the Republic of Serbia to combat cybercrime and emphasise the importance of legal and operational approaches to this issue. They examine the international and national legislative framework, significant crimes, specialised law enforcement agencies and judicial expertise and offer recommendations for improving legislation and institutional processes in this area. The common aspects between the

studies lie in addressing the issue of cybercrime in modern society and emphasising the importance of combating this phenomenon. However, the study on methods to combat cyberterrorism focuses on creating specific methods to counter cyber threats. In contrast, the study by Leštanin and Nikac is centred on the efforts of the Republic of Serbia to combat cybercrime and offers recommendations for improving legislation and institutional processes.

Constantin (2021) highlighted the characteristics of cyber reconnaissance in the online environment and demonstrated how this method could help counter potential cyber-attacks. To emphasise the role of cyber reconnaissance in combating potential threats, the author examined the evolution of terrorism at the European level and discussed how cyber reconnaissance contributed to countering terrorist attacks online. Thus, both studies address the issue of cyberterrorism and identify its increasing prevalence as a method of attack on various organisations. Nevertheless, the study on countering cyberterrorism is focused on analysing cyber-attacks and methods to combat them. At the same time, Constantin's paper pays attention primarily to the evolution of terrorism at the European level and the impact of cyber reconnaissance on countering terrorist attacks.

On the other hand, Broeders *et al*. (2021) conducted an analysis of the evolution and interaction of national policies and international diplomacy in the context of cyberterrorism among the permanent members of the United Nations Security Council (UNSC) and the process of establishing UN norms in the cyber domain. The researchers examined how national policies gradually link cyberterrorism to information security by expanding preventive measures to low-level cyber activities and online content. They also highlighted the question of how diplomatic language on cyberterrorism, due to the adoption of comprehensive and imprecise definitions, may support authoritarian regimes in using counterterrorism measures against internal opposition and vulnerable groups. As a result, it is concluded that in light of the growing debates in the UN on countering (dis)information operations, precise language must be used to ensure global protection of human rights. Thus, both studies analysed cyberterrorism and addressed information security issues in the online space. However, the latter study on cyberterrorism focuses on developing strategies to counter cyberterrorism, while the study of 2021 focuses on analysing diplomatic approaches and formulating norms in this area.

Azzahidi and Junianse (2023) discussed the national security of Indonesia and the European Union (EU) in the context of cyberterrorism. The development of information technologies has changed the nature of attacks on cyberspace, which has become known as cyberterrorism. The study used the theory of cyberterrorism and national security to analyse this issue. The results show that international agreements stimulate Indonesia and the EU to develop cybersecurity laws. The commonality between the studies lies in the discussions of cyberterrorism and the role of international cooperation in combating cyber threats. While the present study focuses on strategies to combat cyberterrorism, the study by Azzahidi and Junianse analysed how international agreements can stimulate the development of legal measures in Indonesia and the EU.

Gonzales' (2022) project focused on the latest developments in cybersecurity as a tool of foreign policy and counterterrorism. Despite potential changes in the nature of the global terrorist threat in recent years, jihadist and separatist groups continue to use the Internet for planning and conducting terrorist attacks and for disseminating their ideology in the online space. Therefore, combating terrorists' Internet use and identifying their communications on various social media and messengers have become priorities for international cooperation. The project examined recent trends and considered various aspects accompanying the complex task of countering terrorism online, including cybersecurity and privacy issues. Both studies addressed cybersecurity issues and its role in combating terrorism, acknowledging the significant impact of the Internet on modern forms of terrorist activities. However, while the mentioned project analysed recent trends in cybersecurity and identified various aspects of countering terrorism online, including privacy and cybersecurity issues, the cyberterrorism study focuses on developing methods to counter cyberterrorism.

Haider (2023) noted that cyberterrorism is using digital technologies for terrorist acts. Cyberterrorists utilise hacking, viruses, DDoS attacks, and information warfare. Their goals include causing damage to systems, stealing information, and spreading fear. The consequences can be severe: economic losses, disruption of services, and security threats. Developing cybersecurity measures is an important task for protecting against cyberterrorism. Thus, both studies emphasise the danger of cyberterrorism and its potential consequences for society. However, the current study focuses on implementing ways to coun-

ter cyber threats, while the researcher's study is focused on describing the problem itself and its consequences.

The study by Prasad and Kumar (2022) also focuses on cyber threats and countermeasures, but in the context of the situation in India. The paper analysed the dangers associated with cyberterrorism and examined the initiatives of the Indian government to counter them. The study aims to understand cyberterrorism and its implications for national security and to assess the effectiveness of the measures taken. The conclusion indicated the need for further action to ensure cybersecurity in India. Thus, both studies address cyber threats and ways to counter them, and analyse the dangers of cyberterrorism. Despite this, they differ in their approaches to assessing consequences and the proposed counteraction strategies based on the unique characteristics of the situations in different countries.

In addition, Mahboob *et al*. (2023) evaluated the state of global law enforcement in combating cyberterrorism and identified the need for new international legal instruments. The research analysed the effectiveness of existing legislative mechanisms in responding to the cyberterrorism threat and considered the possibilities of using new technologies in law enforcement. It also emphasised the importance of international cooperation in strengthening cybersecurity and proposed a comprehensive approach to combating cyber threats. The findings of the work highlight multiple facets of cyber violence and underscore the necessity for coordinated global efforts. Besides, they offer valuable suggestions for crafting novel strategies and enhancing international collaboration to address cyberterrorism. Thus, both studies focus on the importance of international cooperation in combating cyberterrorism and emphasise the need to develop new tools for effective counteraction. However, they differ in research methodology and focus on specific aspects of cybersecurity.

Finally, Renfro (2022) explored the impact of cyberspace on mass violence and terrorism worldwide. The researcher identified the role of the Internet in facilitating terrorist acts and discussed the vulnerability of the USA to such threats. The author noted that the role of cyberspace in the USA is underestimated and requires serious attention. It can be concluded that both studies examine the influence of cyberspace on terrorism, highlighting its pivotal role in facilitating terrorist acts and indicating the vulnerability of countries to such threats. However, the current study focuses on modern forms of cyberterrorism and methods to counteract them, while the research by Renfro discusses a comprehensive strategy for combating terrorism in the USA. In addition, this paper focuses more on specific counteraction strategies, whereas the study of 2022 discusses general trends and areas in international strategy development.

It is important to note that examining cyberterrorism and methods to counteract it is a relevant task in the modern world. Various studies emphasise the need for international cooperation and the development of new strategies for effectively combating cyber threats. The current study presents a structural scheme to systematise the process of countering cyberattacks, focusing on detecting potential attacks, analysing their effectiveness, and planning future steps. It uses real-world examples of global cyberattacks to contextualise the threat and highlight systemic flaws in information security. The study's practical value lies in its recommendations for enhancing cybersecurity at both governmental and corporate levels. It advocates for continuously updating and improving cybersecurity strategies to counter emerging threats and technological developments. The study integrates technical, organisational, and legal measures to ensure information system security and protect digital resources from cyber threats.

Conclusions

The goal of this study was to create practical plans to combat cyberterrorism using contemporary techniques and tools. Python code was created and tested, the key themes and concerns surrounding cyberterrorism were examined, and different forms of cyberterrorism and countermeasures were contrasted.

A thorough strategy to combat cyberterrorism was created due to the investigation, including some techniques and approaches to stop cyber threats. To identify and prevent future cyberattacks, software code was also implemented to analyse network traffic, assess data transfer, and automatically block suspicious activity. The program's output contained details on known cyber threats, offering insightful information for more research and countermeasures. A comparative table of the various forms of cyberterrorism and their attributes was also created as part of the study's scope, which may help in the development of more effective countermeasures as well as improve comprehension and analysis of the problem. Additionally,

a structural diagram detailing a strategy for successfully countering these threats was developed. It started with the identification of possible attacks and ended with an evaluation of the success of the actions taken and the formulation of future plans.

The acquired results are of great practical significance, as they form the basis for creating and applying successful cybersecurity systems at different scales. The software tools and methods developed can help states and organisations improve their cybersecurity posture and lower cyberattack risks. In light of this study's findings, it is advised to conduct more thorough research on contemporary trends in cyberterrorism and constantly enhance strategies for thwarting cyber threats. Additionally, it's critical to keep creating and enhancing software tools for network monitoring and cyberattack defence.

References

AKHMETOV, B.; AIDARKUL, M. (2023). "Modeling of cyber threats in information networks of remote service systems". *The Bulletin of Academy of Logistics and Transport*, vol. 126, no. 3, pp. 306-314. DOI: https://doi.org/10.52167/1609-1817-2023-126-3-306-314

AKYLBAYEVA, I. M.; MALGARAYEVA, Z. B.; KUSSAINOVA, Zh. D.; AMANZHOLULY, S. K.; UMIRZAKOVA, L. A.; KALENOVA, T. S.; ZHARKENOVA, A. M.; TLEBALDIYEVA, M. D. (2014). "Resources of terrorism spread and its globalization". *Life Science Journal*, vol. 11, no. 1s, pp. 202-206 [online]. Available at: https://www.lifesciencesite.com/lsj/life1101s/036_22847life1101s2014_202_206.pdf

ALIMSEITOVA, Zh.; BEKETOVA, G. (2022). "Analysis of neural network models and methods for detecting and recognition of network attacks". *The Bulletin of Academy of Logistics and Transport*, vol. 122, no. 3, pp. 227-236. DOI: https://doi.org/10.52167/1609-1817-2022-122-3-227-236

AMIROVA, A.; TOKHMETOV, A. (2022). "Combined model of threat detection in industrial internet of things". *Bulletin of the Abai Kazakh National Pedagogical University, the Series of "Physical and Mathematical Sciences"*, vol. 77, no. 1, pp. 70-77. DOI: https://doi.org/10.51889/2022-1.1728-7901.09

ARSTANBEKOV, M.; SEIDAKMATOV, N.; TATENOV, M.; KANYBEKOVA, B.; KAKESHOV, B. (2024). "Victimological aspects of countering internet crime: State and local government practices". *Social and Legal Studios*, vol. 7, no. 1, pp. 221-234. DOI: https://doi.org/10.32518/sals1.2024.221

AZZAHIDI, I.; JUNIANSE, F.M. (2023). "Analysis of Indonesian and European Union (EU) relationship strategy overcoming cyber terrorism". *MANU Journal of the Centre for Science and Language Upgrading*, vol. 34, no. 2, pp. 1-16. DOI: https://doi.org/10.51200/manu.v34i2.4767

BORKO, T.; VILKS, A. (2023). "Consequences and threats of international terrorism for Ukraine". *Foreign Affairs*, vol. 33, no. 3, pp. 43-50. DOI: https://doi.org/10.46493/2663-2675.33(3).2023.43-50

BROEDERS, D.; CRISTIANO, F.; WEGGEMANS, D. (2021). "Too close for comfort: Cyber terrorism and information security across national policies and international diplomacy". *Studies in Conflict and Terrorism*, vol. 46, no. 12, pp. 2426-2453. DOI: https://doi.org/10.1080/1057610X.2021.1928887

BUTLER, G.; MONTASARI, R. (2023). "The impact of the Internet on terrorism and violent extremism". In: *Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications*, pp. 427-436. Cham: Springer. DOI: https://doi.org/10.1007/978-3-031-20160-8_24

CANTIKA, S.; UMNIYAH, A. (2023). "Analysis of the Australian government's security strategy in countering the potential threat of terrorism groups through cyber terrorism instruments". *Insignia Journal of International Relations*, vol. 10, no. 2, pp. 214-227. DOI: https://doi.org/10.20884/1.ins.2023.10.2.9376

CERT-UA (2023). *Massive cyberattack UAC-0050 using RemcosRAT/MeduzaStealer against Ukraine and Poland (CERT-UA#8218)* [online]. Available at: https://cert.gov.ua/article/6276652

CONSTANTIN, D.M. (2021). "Cyber intelligence – Method of countering terrorism". *Researchgate* [online]. Available at: https://www.researchgate.net/publication/370520729_CYBER_INTELLIGENCE_-METHOD_OF_COUNTERING_TERRORISM

GONZALES, D. (2022). "It's getting harder to do: Countering terrorist use of the Internet". In: *Terrorism and Transatlantic Relations*, pp. 165-190. Cham: Palgrave Macmillan. DOI: https://doi.org/10.1007/978-3-030-83347-3_8

HAIDER, A. (2023). "Cyber terrorism". *Researchgate* [online]. Available at: https://www.researchgate.net/publication/375895130_alarhab_alsybrany_Cyber_Terrorism

KALMURZAEV, B. A.; OZKAN, O.; RAZDYKOVA, G. M.; BEKBOSYNOV, E. T. (2021). "Comparative legal analysis of national legislation on countering religious extremism with the national legislation of foreign countries". *Bulletin of the Toraighyrov University*, no. 4, pp. 9-23. DOI: http://doi.org/10.48081/LOOG2605

KANYBEKOVA, B.; ARSTANBEKOV, M.; KAKESHOV, B.; ERDOLATOV, C. S.; ARTYKBAEV, I. (2023). "Criminological aspects of the behaviour of victims of cyberattacks: Case analysis of hacking state organisations ensuring national security". *Pakistan Journal of Criminology*, vol. 15, no. 4, pp. 175-192.

KIM, S. (2024). "Chinese hackers controlled critical IT infrastructure in Kazakhstan". *Factcheck* [online]. Available at: https://factcheck.kz/novosti/kitayskie-hakery-kontrolirovali-kriticheskie-obekty-it-infrastruktury-kazahstana

LEŠTANIN, B.; NIKAC, Z. (2022). "Fight against cyber crime in Republic of Serbia". In: *International Crime and Punishment Film Festival "Justice in the Virtual World"*, pp. 65-78 [online]. Available at: https://www.academia.edu/42755559/FIGHT_AGAINST_CYBER_CRIME_IN_REPUBLIC_OF_SERBIA

MAHBOOB, S. M.; ABBAS, S. S.; SHAHEEN, I. A. (2023). "Adapting to cybersecurity challenges: Assessing the effectiveness of international law against cyber terrorism". *Journal of Social Research Development*, vol. 4, no. 4, pp. 669-685. DOI: https://doi.org/10.53664/JSRD/04-04-2023-02-669-685

METELSKYI, I.; KRAVCHUK, M. (2023). "Features of cybercrime and its prevalence in Ukraine". *Law, Policy and Security*, vol. 1, no. 1, pp. 18-25.

MONTASARI, R. (2024). "Analysing ethical, legal, technical and operational challenges of the application of machine learning in countering cyber terrorism". In: *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution*, pp. 159-197. Cham: Springer. DOI: https://doi.org/10.1007/978-3-031-50454-9_9

MOVCHAN, A.; SHLIAKHOVSKYI, O.; KOZII, V.; FEDCHAK, I. (2023). "Investigating cryptocurrency financing crimes terrorism and armed aggression". *Social and Legal Studios*, vol. 6, no. 4, pp. 123-131. DOI: https://doi.org/10.32518/sals4.2023.123

OSPANOVA, A.; ZHARKIMBEKOVA, A.; KUSEPOVA, L.; TOKKULIYEVA, A.; MANMURYN, M. (2021). "Cloud service for protection and monitoring of computer networks". *Engineering Journal of Satbayev University*, vol. 143, no. 3, pp. 222-229. DOI: https://doi.org/10.51301/vest.su.2021.i3.29

PRASAD, S.; KUMAR, A. (2022). "Cyber terrorism: A growing threat to India's cyber security". In: *Nontraditional Security Concerns in India*, pp. 53-73. Singapore: Palgrave Macmillan. DOI: https://doi.org/10.1007/978-981-16-3735-3_4

RENFRO, E. (2022). "Messengers of death: Cyber and the root structure of terror". In: *Research Anthology on Modern Violence and Its Impact on Society*, pp. 582-599. Hershey: IGI Global. DOI: https://doi.org/10.4018/978-1-6684-7464-8.ch032

SALIH, A. J.; AL ALAZZAM, F. A. (2023). "A competent approach to the training of lawyers in "cyberterrorism"". *Pedagogy and Education Management Review*, no. 1, pp. 29-43. DOI: https://doi.org/10.36690/2733-2039-2023-1-29

SANGER, D.; KRAUSS, C.; PERLROTH, N. (2021). "Cyberattack forces a shutdown of a top U.S. pipeline". *The New York Times* [online]. Available at: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

SHOPINA, I.; KHOMIAKOV, D.; KHRYSTYNCHENKO, N.; ZHUKOV, S.; SHPENOV, D. (2020). "Cybersecurity: Legal and organizational support in leading countries, NATO and EU standards". *Journal of Security and Sustainability Issues*, vol. 9, no. 3, pp. 977-992. DOI: https://doi.org/10.9770/jssi.2020.9.3(22)

SIDDHA, A.; BENARRIVO, R. (2023). "Counter cyber terrorism governance in Indonesia". *Khazanah Sosial*, vol. 5, no. 2, pp. 359-367. DOI: https://doi.org/10.15575/ks.v5i2.26414

SOPILKO, I.; RAPATSKA, L. (2023). "Social-legal foundations of information security of the state, society and individual in Ukraine". *Scientific Journal of the National Academy of Internal Affairs*, vol. 28, no. 1, pp. 44-54. DOI: https://doi.org/10.56215/naia-herald/1.2023.44

TYMOSHENKO, V. (2022). "Terrorism as a threat to human rights". *Law Journal of the National Academy of Internal Affairs*, vol. 12, no. 3, pp. 30-38. DOI: https://doi.org/10.56215/04221203.30

VILKS, A.; KIPANE, A.; KUDEIKINA, I.; PALKOVA, K.; GRASIS, J. (2022). "Criminological aspects of current cyber security". *Revista de Direito, Estado e Telecomunicacoes*, vol. 14, no. 2, pp. 94-108. DOI: https://doi.org/10.26512/lstr.v14i2.41411

Recommended citation

BISHMANOV, Kakimzhan; MURATZHAN, Zarina; DILBARKHANOVA, Zhanat; LYUTSIK, Viktoriya (2024). "Analysis of modern types of cyberterrorism and methods for countering them". *IDP. Internet, Law and Politics Journal*, no. 41. UOC [Accessed: dd/mm/yy]. http://dx.doi.org/10.7238/idp.v0i41.428542

About the authors

Kakimzhan Bishmanov
Al-Farabi Kazakh National University
kakimzhan53bishmanov@gmail.com
ORCID: https://orcid.org/0009-0007-4344-9800

PhD in Law, Professor at the Department of Cultural and Religious Studies, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan. His scientific interests include cybersecurity, modern forms of cyberattacks and effective countermeasures.

Zarina Muratzhan
M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan
z.muratzhan@proton.me
ORCID: https://orcid.org/0009-0002-2008-8225

Researcher at the M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Almaty, Republic of Kazakhstan. Her research interests include information security and efficient strategies for countering contemporary cyber threats.

Zhanat Dilbarkhanova
M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan
dilbarkhanova.law@hotmail.com
ORCID: https://orcid.org/0009-0004-8917-8741

Full Doctor in Law, Deputy Chief of the M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Almaty, Republic of Kazakhstan. Her scientific interests include improving cybersecurity, computer attack protection and software implementation of cybersecurity strategies.

Viktoriya Lyutsik
Turan University
vita_lyutsik@protonmail.com
ORCID: https://orcid.org/0009-0002-6272-2212

PhD in Law, Associate Professor at the Department of Jurisprudence and International Law, Turan University, Almaty, Republic of Kazakhstan. Her scientific interests include security, digital threats, combating cyber threats and addressing global cyberattacks.