Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:1530
doi: 10.56294/sctconf20251530

ORIGINAL

The impact of biometric technologies on the efficiency of terrorist crime investigation

El impacto de las tecnologías biométricas en la eficacia de la investigación de los delitos de terrorismo

Yevhen Bondarenko[1], Ivo Svoboda[2], Ivan Tkachov[3], Oleksandr Kozenko[3], Volodymyr Vislovukh[4]

[1]Department of Law Enforcement and Anti-Corruption Activities, Educational and Scientific Institute of Law Prince Vladimir the Great, Interregional Academy of Personnel Management. Kyiv, Ukraine.
[2]AMBIS. Prague, Czech Republic.
[3]Scientific Laboratory of National Academy, Security Service of Ukraine. Kyiv, Ukraine.
[4]Department of the National Academy, Security Service of Ukraine. Kyiv, Ukraine.

Cite as: Bondarenko Y, Svoboda I, Tkachov I, Kozenko O, Vislovukh V. The impact of biometric technologies on the efficiency of terrorist crime investigation. Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:1530. https://doi.org/10.56294/sctconf20251530

Submitted: 30-08-2024 **Revised:** 29-11-2024 **Accepted:** 23-02-2025 **Published:** 24-02-2025

Editor: Prof. Dr. William Castillo-González

Corresponding Author: Yevhen Bondarenko

ABSTRACT

Introduction: the relevance of biometric technology in investigating terrorist crimes is increasing due to the rise in global security threats and the need to enhance law enforcement effectiveness. The main goal of this article is to evaluate how biometric technologies enhance the identification, tracking, and prevention of terrorist activities globally.
Method: the research methodology includes statistical data analysis, calculation of weighted averages, and scenario forecasting concerning terrorist attacks. The research methodology involves statistical analysis of terrorism-related data, weighted average calculations, and scenario-based forecasting to assess biometric technology applications.
Results: the study identifies key factors associated with biometrics, including facial recognition, fingerprint analysis, and retinal scanning technologies, and outlines their potential impact on increasing crime-solving rates. The results show that the use of biometric systems significantly reduces the number of unsolved terrorist crimes, enhances law enforcement coordination, and aids in early threat prevention.
Conclusions: the article discusses various challenges countries face in solving crimes, such as underdeveloped infrastructure and inadequate adoption of modern technologies. The practical significance of the study lies in providing recommendations to improve international cooperation and further implement biometric technologies to ensure global security. Future research should focus on exploring new ways of integrating biometric technologies into law enforcement systems and adapting them to evolving threats.

Keywords: Biometric Technologies; Terrorist Crimes; Criminal Investigation; Global Security; International Cooperation; Law Enforcement; Terrorism Prevention.

RESUMEN

Introducción: la relevancia de la tecnología biométrica en la investigación de delitos terroristas es cada vez mayor debido al aumento de las amenazas a la seguridad mundial y a la necesidad de mejorar la eficacia de las fuerzas de seguridad. El objetivo principal de este artículo es analizar la aplicación de las tecnologías biométricas para mejorar la eficacia en la detección y detención de terroristas en distintas regiones del mundo.
Método: la metodología de investigación incluye el análisis estadístico de datos, el cálculo de medias ponderadas y la previsión de escenarios relativos a atentados terroristas.

Resultados: el estudio identifica los factores clave asociados a la biometría, incluidas las tecnologías de reconocimiento facial, análisis de huellas dactilares y escaneo de retina, y esboza su impacto potencial en el aumento de los índices de resolución de delitos. Los resultados muestran que el uso de sistemas biométricos reduce significativamente el número de delitos terroristas sin resolver, mejora la coordinación de las fuerzas del orden y ayuda a la prevención temprana de amenazas.
Conclusiones: el artículo analiza diversos retos a los que se enfrentan los países a la hora de resolver delitos, como el subdesarrollo de las infraestructuras y la adopción inadecuada de tecnologías modernas. La importancia práctica del estudio radica en que ofrece recomendaciones para mejorar la cooperación internacional y seguir aplicando las tecnologías biométricas para garantizar la seguridad mundial. Las investigaciones futuras deberían centrarse en explorar nuevas formas de integrar las tecnologías biométricas en los sistemas de aplicación de la ley y adaptarlas a la evolución de las amenazas.

Palabras clave: Tecnologías Biométricas; Delitos Terroristas; Investigación Criminal; Seguridad Global; Cooperación Internacional; Aplicación de la Ley; Prevención del Terrorismo.

INTRODUCTION

The quality of investigating terrorist crimes remains one of the most complex issues in global security. Detection and prevention are complicated by the multi-component nature of terrorist acts. It's involve perpetrators and financiers operating through criminal organizations with resources spread across various countries. Terrorists coordinate through complex digital networks in countries with vulnerable security systems. Many terrorist groups use anonymous platforms for communication and financing, complicating their detection and identification. One of the greatest challenges is the lack of effective early detection methods, which limits the ability to prevent attacks before they occur.

A significant number of terrorist crimes remain unsolved due to insufficient coordination among law enforcement agencies in different countries. Consequently, the masterminds behind terrorist attacks often remain undetected, posing a continuous threat to global security. Improving the quality of investigations and preventing terrorist acts requires new approaches to actively use modern technologies, as biometric systems can significantly enhance the precision and speed of detecting terrorists.

International cooperation among organizations in terrorist crime investigations is essential for combating global terrorism, as no single country can tackle this issue alone. Organizations like Interpol, Europol, and the United Nations actively promote collaboration by facilitating intelligence sharing and assisting in identifying criminal networks. The Counter-Terrorism Partnership Fund program is particularly important, helping strengthen countries' anti-terrorism capabilities through technical support and enhanced law enforcement training.

One of the key achievements of international cooperation is the creation of global databases that compile information on individuals potentially involved in terrorist attacks, allowing faster identification and prevention of future attacks. International organizations enable joint operations to identify and neutralize terrorist groups. Between 2010 and 2023, Interpol-led operations resulted in the arrest of thousands of terrorists and the disruption of over a hundred criminal organizations. International cooperation helps establish an early-warning system for terrorist threats, though questions of control and functionality remain open to debate.

Recently, the acceleration of digitalization has played a decisive role in improving the investigation of terrorist crimes, with biometric technologies becoming one of the key tools in this process. In today's world, terrorists actively use digital platforms to organize their activities, complicating detection with traditional investigation methods. Biometrics opens new opportunities for law enforcement in combating terrorism. The Clearview AI system in the United States allows the instant identification of individuals suspected of terrorism through facial analysis from social media photos.

These technologies speed up the identification and apprehension process, reducing the time from threat detection to neutralization. Biometric systems can also be used to monitor suspicious individuals at borders and in international airports, enhancing security globally. Iris ID systems are widely used to protect critical infrastructure and access to secure facilities, making terrorist attacks less likely. With the rapid implementation and constant improvement of biometric technologies, a significant reduction in terrorist attacks and improved investigation efficiency can be expected in the future.

The aim of the study is to analyze the impact of biometric technologies on the effectiveness of investigating terrorist crimes in the context of modern digitalization and global security. This study aims to assess the role of biometric technologies in improving the investigation and prevention of terrorist crimes amid modern digitalization and global security challenges. The following objectives were defined to achieve this goal:

1. Analyze global trends in terrorist crimes up to 2022 and identify major trends in their investigation.
2. Investigate current biometric technologies and their role in detecting and identifying terrorism suspects.

https://doi.org/10.56294/sctconf20251530

3. Determine the world's most dangerous regions based on terrorism indices and assess the applicability of biometric technologies in these countries.

Literature review

The issue of implementing biometric technologies in terrorist crime investigations is becoming increasingly relevant due to the growing global terrorism threat and the need to enhance law enforcement efficiency. Researcher Hrabchuk[1] emphasizes that using facial recognition biometric systems significantly reduces the time needed to identify criminals. Hegghammer's[2] work explores the impact of fingerprint recognition technology on improving the overall level of terrorist attack detection in Europe. Hakim[3] highlights the importance of biometric data exchange between countries to prevent international terrorist crimes. Apak's[4] study addresses the role of retinal recognition systems in protecting critical infrastructure, noting their high accuracy in identifying suspects. Paul[5] analyzes the effectiveness of cooperation between law enforcement agencies in the United States and the European Union in the context of biometric data exchange.

Grünenberg[6] addresses challenges in implementing biometric technologies in countries with low levels of digital infrastructure, where access to such technology is limited. Shanaah[7] examines the use of biometric systems to monitor suspicious individuals at international airports, underscoring the importance of this tool in preventing terrorist attacks. Erol[8] highlights the necessity of international cooperation in developing unified standards for biometric data exchange between countries. Rothenberger[9] discusses the prospects of using artificial intelligence combined with biometric technologies to predict terrorist threats, enabling timely detection of potential attacks. Li[10] suggests that modern voice recognition systems can be used in counter-terrorism efforts, especially to identify criminals based on intercepted conversations. Brodén's[11] research evaluates the effectiveness of biometric technology implementation in Africa and the Middle East, where terrorism remains a serious threat to regional security.

The studies by Bulavina et al.[12] and Trokhymenko et al.[13] emphasize the role of modern technology in strategic analysis, which is important for the effective use of biometric systems in terrorism investigations. The paper by Voloshanivska et al.[14] examines the link between corruption and criminal networks that use fake documents to evade justice. An analysis by Kniaziev et al.[15] shows that methods of combating manipulation in sports can be adapted to investigate terrorist financing schemes. The article of Kozachenko et al.[16] discusses international cooperation in criminal investigations, which is important for integrating biometric data into the law enforcement system. The study by Ishchenko et al.[17] examines the psychological aspects of identifying individuals in crises, which can be useful in profiling suspects. Valyukevych et al.[18] analyze the use of speech analysis software that can complement biometric methods of identifying terrorists.

Equatora's et al.[19] work examines privacy and ethics issues in using biometric systems within law enforcement, stressing the importance of data protection in conducting terrorist investigations. Thus, scholars agree that biometric technologies are an important tool in combating terrorism, yet their implementation requires significant coordination between countries, infrastructure development, and legal support. Future research should address the issue of regulatory and legal frameworks for biometric technology applications from ethical and legal perspectives.

METHOD

Research procedure

The initial stage of the research procedure involved analyzing the global count of terrorist attacks up to 2022. For this purpose, statistical data were gathered from the Global Terrorism Database on terrorist crimes from 2007 to 2022.[20] The next step identified the world's most dangerous countries according to the Terrorism Index for 2023, highlighting regions with the highest threats, such as Burkina Faso, Israel, Mali, Afghanistan, and others. The study examined which biometric technologies can detect threats and identify suspects. Subsequently, an analysis of the number of solved terrorist crimes in various regions was conducted, forming an overall average detection rate. The final stage projected the effectiveness of biometric technologies in investigating terrorist crimes, considering the potential increase in their use in the future.

Sample formation

The study sample included 20 countries with a high terrorism index of over 5 points as of 2023 (table 1). The general population comprised Israel, Syria, Egypt, and Pakistan, given their high terrorist activity levels. These countries pose the most significant threat to global security, making it essential to examine their situations closely. For the analysis, biometric technologies actively used for criminal identification were selected: facial recognition—Clearview AI, fingerprints—AFIS, retina analysis—Iris ID, and voice recognition—Nuance Dragon. These technologies were chosen for their high accuracy and application in international crime investigations.

https://doi.org/10.56294/sctconf20251530

Methods

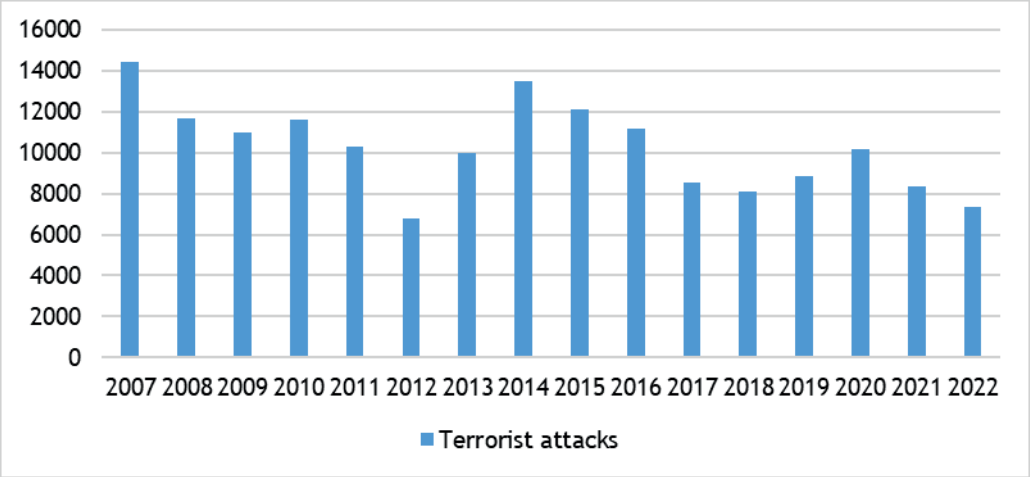
Various analytical methods were applied in the study to understand the impact of biometric technologies on investigating terrorist crimes. The main method was a statistical analysis of the number of terrorist attacks and scenario forecasting. A weighted average calculation assessed the average detection rate of terrorist crimes in different world regions. Scenario forecasting predicted the impact of biometric technologies, considering their potential development and implementation by 2032. A comparative method analyzed the effectiveness of biometric technologies in countries with varying levels of digital infrastructure and economic development. Data were collected from secondary sources, and the applied methodology ensures the study's replicability.

Tools

Statistical tools such as SaS were used to analyze secondary data from reports by international security organizations like the Federal Bureau of Investigation (FBI) and Europol. The analysis also included judicial data from countries with high terrorist activity levels. Open data provided a realistic picture of the current state of counterterrorism. Excel was used to process statistical data, create charts visualizing the dynamics of terrorist attacks, and display detection rates using biometric technologies.

RESULTS

Terrorism has significantly intensified in the 21st century, becoming a powerful means of political struggle used by radical groups to achieve ideological or geopolitical goals. Over recent decades, terrorism has become one of the main threats to countries with developed infrastructures. In the current geopolitical situation, terrorist groups employ both traditional military tactics and advanced technologies, including cyberterrorism, to carry out attacks. Events from 2020 to 2024, such as terrorist acts in Europe like the 2020 Vienna attack, show that terrorism remains a significant threat to the global community. With advancing technologies, terrorist attacks are becoming increasingly complex, necessitating new approaches by governments to counter this threat. The overall trend in terrorist attacks is illustrated in figure 1.



Source: compiled based on Statista data[21]

Figure 1. Number of terrorist attacks worldwide between 2007 and 2022

The dynamics of terrorist attacks from 2007 to 2022 indicate significant fluctuations in the number of incidents, driven by social-political and economic factors. In 2007, there were 14 414 recorded terrorist attacks, which dropped to 11 662 in 2008. Overall, from 2007 to 2012, there was a gradual decrease, reaching a low in 2012 with 6 771 attacks. However, from 2013, due to the activation of terrorist groups in the Middle East, particularly ISIS, the number of attacks sharply increased, peaking in 2014 with 13 482 incidents.

This period was marked by intensifying conflicts in Syria, Iraq, and other countries in the region. The number of attacks subsequently declined, reaching 8 548 in 2017 as a result of the active counterterrorism efforts by the international coalition. In 2022, the number of attacks further decreased to 7 342; however, this does not indicate a complete victory over terrorism but rather a shift in terrorist groups' tactics and improved countermeasures.

Countering terrorism remains a high priority for most countries, as the threat of terrorist attacks persists. Many states have developed strategies for combatting terrorism, including military and intelligence measures aimed at prevention and neutralization. Key methods of counterterrorism include international security cooperation, intelligence sharing, the use of advanced technologies, and the strengthening of domestic security. The largest hubs of terrorism are in regions with high political instability, such as the Middle East, North Africa, and Afghanistan. Syria, Iraq, Nigeria, and Afghanistan continue to be the primary areas of terrorist activity.

https://doi.org/10.56294/sctconf20251530

However, terrorist attacks are not confined to these regions; Europe and the United States also remain targets, necessitating ongoing security enhancements. The internationalization of terrorist threats, including cyberterrorism, renders terrorism a global issue requiring coordinated action from all countries. The most dangerous countries by the terrorism index are listed in table 1.

Table 1. The most dangerous countries according to the terrorism index, 2023

Rank	Region	Score
1	Burkina Faso	8,571
2	Israel	8,143
3	Mali	7,998
4	Pakistan	7,916
5	Syria	7,89
6	Afghanistan	7,825
7	Somalia	7,814
8	Nigeria	7,575
9	Myanmar	7,536
10	Niger	7,274
11	Iraq	7,078
12	Cameroon	6,98
13	Democratic Republic of the Congo	6,514
14	India	6,324
15	Mozambique	6,267
16	Colombia	6,188
17	Chile	5,679
18	Kenya	5,616
19	Philippines	5,383
20	Egypt	5,221

Source: compiled based on Vision of Humanity[22]

One of the key challenges in combating terrorism is the vulnerability of countries with low economic development and limited digital infrastructure. This hinders the use of biometric technologies to prevent terrorist acts. According to the 2023 Global Terrorism Index, the most dangerous countries remain Burkina Faso (8571 points), Mali (7998), and Pakistan (7916). In these countries, the level of digital infrastructure remains low, complicating the implementation of modern technologies for security purposes. In Afghanistan (7,825), the lack of political stability and economic support hinders the creation of centralized databases for tracking individuals associated with terrorist groups. Somalia (7814) and Nigeria (7575) face issues with corruption and unstable governance, further hindering the effective use of advanced technologies. The limited implementation of biometric systems significantly reduces the chances for timely prevention and investigation of terrorist acts, increasing the overall risk in these countries.

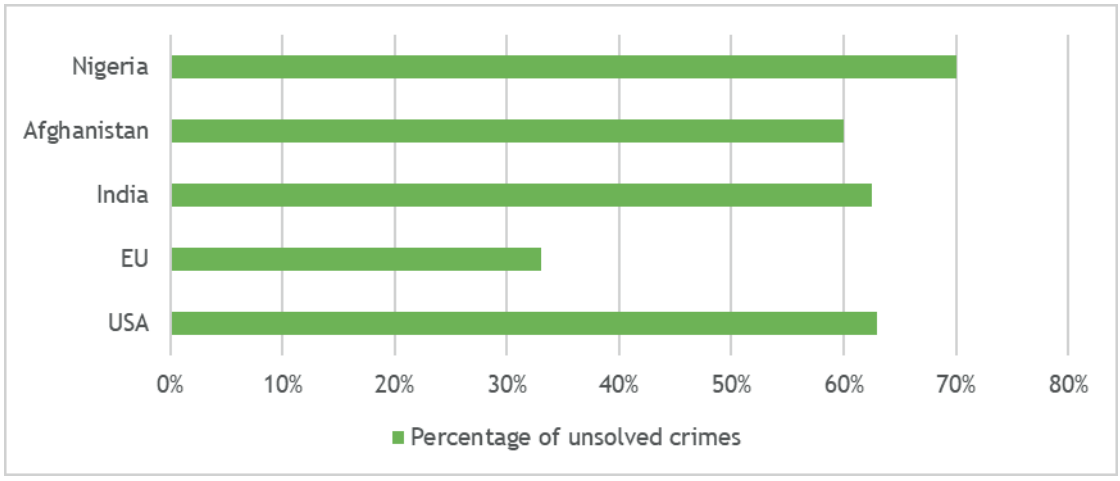
International cooperation in detecting and investigating terrorist acts has become a key element in the fight against global terrorism. One of the most important examples is the participation of states in the Global Coalition against ISIS, founded in 2014 and involving over 80 countries. The main goal of the coalition is to exchange intelligence, coordinate military operations, and support countries affected by terrorist attacks. Interpol plays an essential role in international cooperation by providing data exchange opportunities through specialized databases on individuals who may be involved in terrorist activities.

An example of using biometric technologies is the Secure Information Exchange Network Application (SIRENE), which facilitates European information exchange about criminals and suspects, including biometric data. The U.S. actively collaborates with Europe through the Counter-Terrorism Partnership Fund, which finances projects to ensure international information exchange for early detection of terrorist threats. Joint use of biometric systems allows for quicker identification of criminals and successful operations to apprehend them. Key examples are listed in table 2.

https://doi.org/10.56294/sctconf20251530

Table 2. Biometric technologies for investigating terrorist crimes

Technology Name	System/Program	Description	Technical Parameters
Face Recognition	Clearview AI	Database for facial recognition using analysis of billions of images	Accuracy: 99 %, Processing Time: 1 sec, Database Capacity: over 3 billion faces
Fingerprint Biometrics	AFIS (Automated Fingerprint Identification System)	Automated identification system based on fingerprints	Accuracy: 98 %, Analysis Speed: 2 sec
Voice Recognition	Voice Recognition	Voice Recognition	Voice Recognition
Retina Recognition	Iris ID (IrisAccess)	System for retina recognition using multi-factor identification	Accuracy: 99 %, Processing Time: 3 sec
Gait Recognition	AI Gait Recognition by Watrix	Chinese technology for gait analysis based on surveillance camera footage	Accuracy: 93 %, Processing Time: 5 sec
DNA Analysis	CODIS (Combined DNA Index System)	U.S. national system for DNA storage and analysis	Accuracy: 99,9 %, Processing Time: up to 48 hours
Vein Scanners	Hitachi VeinID	Vein recognition system using infrared hand scanners	Accuracy: 97 %, Processing Time: 2 sec



Source: based on Interpol data[23]

Figure 2. The percentage of unsolved crimes in the regions of the world

Expanding the practice of strengthening control and data exchange between countries is one of the main strategies in the fight against terrorism. One successful example is the Suspicious Person Identification and Data Sharing Program between the U.S. and the EU, which includes mandatory biometric data exchange on individuals suspected of terrorism. This allows countries to identify potential threats early and take preventive measures. Through cooperation between the U.K. and U.S. security services in 2021, a terrorist organization planning attacks in Europe was identified using facial recognition biometric data.

Europol actively uses monitoring and information-sharing programs such as the Terrorist Finance Tracking Program (TFTP), which identifies financial transactions related to terrorist groups. Known successful operations conducted under the Global Aviation Security Plan (GASeP) enhance the capabilities of countries to detect potential terrorists in advance. This is achieved through flight data analysis and the use of biometric technologies at international airports, reducing the level of terrorist threats and strengthening control over criminal groups internationally.

Information on the 63 % of unsolved violent crimes in 2022 is based on data collected by the FBI. The organization uses a crime reporting system that collects information from local, state, and federal law enforcement agencies across the country. According to these data, only 37 % of violent crimes were solved, meaning that 63 % remained unsolved. This indicates significant challenges faced by law enforcement in investigating crimes, including the complexity of gathering evidence, identifying suspects, and securing witness testimony. The general trend of an increase in unsolved crimes may be related to various factors, from the rising number of crimes to limitations in law enforcement resources. The use of biometric technologies and other modern investigative methods may help reduce this percentage in the future. However, achieving this requires adequate funding, personnel training, and the implementation of advanced technologies. The general trend in unsolved crimes is shown in figure 2.

The average percentage of unsolved terrorist crimes in the studied countries is 57,7 %. Such a high figure can be explained by several factors. Terrorist crimes often occur in conditions of high secrecy and careful planning,

complicating the gathering of evidence and identification of suspects. Terrorists may use advanced technologies and methods to avoid detection, further complicating the work of law enforcement. Limited resources and insufficient funding for law enforcement agencies may result in a shortage of personnel and technical means for effective investigation. The international nature of many terrorist groups requires coordination between various countries and organizations, which can be challenging and not always effective.

The high level of unsolved terrorist crimes, which reaches up to 60 % in some countries, remains a serious problem for law enforcement and security services. The causes of this phenomenon vary, but the main factors are the complexity of organizing terrorist groups, their mobility, and the use of modern technologies for coordination. In the U.S., India, and Afghanistan, unsolved crimes exceed 60 %. This is due to the imperfections in existing security systems, the insufficient level of information exchange between law enforcement agencies, and the complexity in identifying individuals involved in terrorist attacks. Even in the age of digitalization, where the use of modern technologies for crime monitoring and investigation is growing, significant problems remain with the accuracy of criminal identification.

The presence of a large number of fake documents, anonymous communication channels, and the use of digital technologies by terrorists to evade pursuit make the crime-solving process difficult and lengthy. Solving this problem may involve actively using biometric technologies, strengthening international cooperation in intelligence sharing, which will significantly increase the rate of solving terrorist acts.

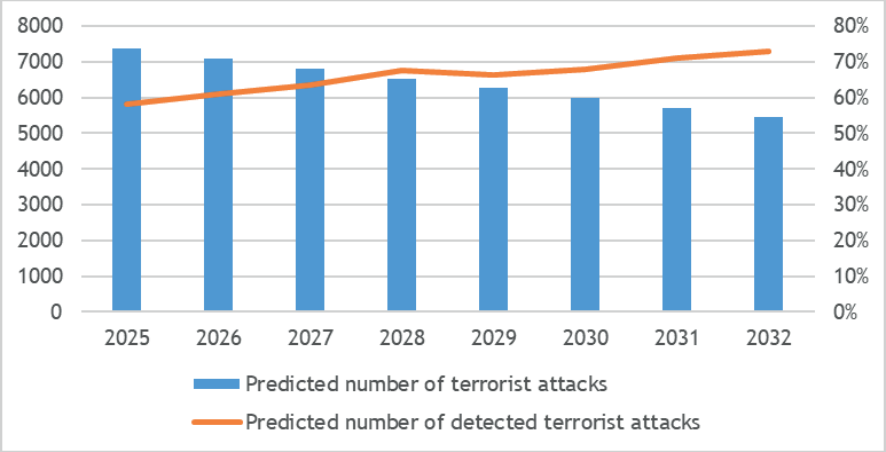


Figure 3. Projected number of terrorist attacks of solved crimes

The application of biometric technologies can significantly reduce the number of terrorist attacks and increase crime detection rates. According to forecasts, with active use of biometric systems, the number of terrorist attacks could decrease to 7 357 cases by 2025, while the crime detection rate would increase to 58 %. In the future, with technology advancements and the implementation of biometric databases, the detection rate could rise to 73 % by 2032, and the number of attacks could fall to 5 437. The unique advantage of biometric technologies lies in their ability to provide accurate information about an individual, allowing for quick identification of suspects. This is especially important under modern terrorist threats, where response speed is critical. Using up-to-date systems enables law enforcement agencies to prevent terrorist acts and promptly apprehend those involved in planning and executing crimes. Thus, biometric technologies may become one of the key tools in combating terrorism.

DISCUSSION

The research findings indicate that biometric technologies significantly enhance the effectiveness of terrorism investigations. This is supported by Sricharan et al.[24], who found that facial recognition enables faster identification of suspects. Our results align with Mijalković et al.[25], who asserts that fingerprint systems increase the detection rate of terrorist crimes. However, Green[26] notes that in countries with limited digital infrastructure, implementing such technologies faces challenges, highlighting the need for international support. Our study also corroborates Pettinger[27], showing that international biometric data sharing accelerates the detection of criminal groups. Additionally, Ghalib[28] confirms that using biometrics at airports substantially improves security, a finding consistent with our results on the effectiveness of such systems in transport hubs.

Shivdas[29] investigates the impact of digitalization and biometric technologies on modern crime investigation methods in Europe and North America. Garciandía's[30] scientific work examines the challenges of implementing biometric technologies in the fight against terrorism in countries with low levels of digital infrastructure development. La Fors[31] highlights that the successful application of biometric systems largely depends on the resources available to support such technology and the political stability of regions.

https://doi.org/10.56294/sctconf20251530

Malik et al.[32] raises ethical challenges associated with biometric data, a crucial issue for our study. Ahmed[33] points out that legislative barriers in some countries may limit biometric system use, necessitating further research. Movchan et al.[34] supports our findings by indicating that combining biometric technologies with automation enhances threat detection and prevention. Patel[35] emphasizes that implementing biometric technologies requires specialized training for law enforcement, consistent with our results. Benamara[36] highlights the importance of centralized databases for counter-terrorism efficiency, which aligns with our conclusions and other researchers' findings. Thus, biometric technologies play a vital role in modern terrorism investigation methods, although substantial infrastructure and legal enhancements are necessary for optimal use. Practical applications of these technologies could also aid in preventing minor crimes and securing crowded areas and critical infrastructure.

Limitations

Despite the comprehensiveness of this study, limitations exist in combining biometric methods with other methods for detecting and preventing terrorism and investigating related cases. This may create additional factors affecting investigation effectiveness, warranting further research. The study should also focus on regions with both highly developed and less developed digital infrastructures for completeness.

CONCLUSIONS

In conclusion, implementing biometric technologies in terrorism investigations is key to enhancing counter-terrorism effectiveness in today's global security landscape. The analysis showed that using biometric systems for suspect identification significantly increases crime detection rates and allows law enforcement to respond more rapidly to threats. Centralized database tools ensure accurate suspect identification and improve coordination among law enforcement agencies. Countries that actively employ these approaches may reduce terrorism rates and improve overall population security.

The most effective counter-terrorism approach involves ensuring international cooperation and focusing on a long-term strategy with a technological infrastructure component. To maximize the efficiency of these approaches, countries should invest in digital infrastructure and data security. Global challenges include ethical use of biometric data and ensuring citizen privacy, as digitalization growth creates new risks in data protection. Future research should focus on counterintelligence methods like DeepFake and broader use of artificial intelligence for terrorism prevention based on biometric technologies.

RECOMMENDATIONS

Based on the research, the following measures are proposed:

1. Develop an integrated strategy for implementing biometric technologies, combining their use with international cooperation and data exchange between law enforcement agencies across countries.
2. Invest in digital infrastructure development in high-threat countries, enabling access to biometric systems and enhancing security in these regions.
3. Support the creation of global centralized databases that enable rapid identification of terrorism suspects, particularly at international transportation hubs and borders.

BIBLIOGRAPHIC REFERENCES

1. Hrabchuk I, Kusiak, D, Makukha, R. Digital tools in anti-money laundering and combating the financing of terrorism: Main characteristics. Herald UNU International Economic Relations and World Economy, 2023;47. https://doi.org/10.32782/2413-9971/2023-47-4

2. Hegghammer Th, Ketchley N. Plots, attacks, and the measurement of terrorism. Journal of Conflict Resolution, 2023;69(1). https://doi.org/10.1177/00220027231221536

3. Hakim L. The problem of the application of the doctrine of inclusion in the eradication of terrorism in Indonesia. SASI, 2023;29(2):286. https://doi.org/10.47268/sasi.v29i2.1344

4. Apak R, Üzer A, Sağlam Ş, Arman A. Selective electrochemical detection of explosives with nanomaterial based electrodes. Electroanalysis, 2023. https://doi.org/10.1002/elan.202200175

5. Paul JA, Bagchi A. Immigration, terrorism, and the economy. Journal of Policy Modeling, 2023;45(3):538-551. https://doi.org/10.1016/j.jpolmod.2023.03.002

6. Grünenberg K. Wearing someone else's face: Biometric technologies, anti-spoofing and the fear of the unknown. Ethnos, 2022;87(2):223–240. https://doi.org/10.1080/00141844.2019.1705869

7. Shanaah S. Explaining the variation and contestation of P/CVE policies around the world: A public policy approach. Critical Studies on Terrorism, 2023;16(3):475–500. https://doi.org/10.1080/17539153.2023.2234708

8. Erol F. Terrorism mortality salience manipulation: A causal mediation analysis. Terrorism and Political Violence, 2023;35(7):1536–1555. https://doi.org/10.1080/09546553.2022.2060081

9. Rothenberger L. Terrorism as communication: Stocktaking, explanations and challenges. Thuringia: Springer Fachmedien Wiesbaden, 2023. https://doi.org/10.1007/978-3-658-38242-1

10. Li, L, Lyu, X, Liang S, Liu, Zh. Application of fluorescence sensing technology in trace detection of explosives. Dyes and Pigments, 2023;220. https://doi.org/10.1016/j.dyepig.2023.111651

11. Brodén D, Olsson L-J, Fridlund M, Ängsal MP, Öhberg P. Diachrony of the new political terrorism. Neologisms as discursive framing in swedish parliamentary data 1971–2018. Digital Humanities in the Nordic and Baltic Countries Publications, 2023;5(1):79–89. https://doi.org/10.5617/dhnbpub.10651

12. Bulavina O, Kyslenko DP, Hmil-Chuprina V, Artemenko S, Cherednyk, L. Efficiency of virtual reality technologies in the development of strategic thinking of future professionals. Journal of Theoretical and Applied Information Technology, 2024;102(18):6750-6760.

13. Trokhymenko G, Litvak S, Litvak O, Andreeva A, Rabich O, Chumak L, Nalysko M, Troshyn M, Komarysta B, Sopov, D. Assessment of iron and heavy metals accumulation in the soils of the combat zone. Eastern-European Journal of Enterprise Technologies, 2023;5(10(125)):6–16. https://doi.org/10.15587/1729-4061.2023.289289

14. Voloshanivska T, Shchokin RH, Pavlova O, Frantsuz AY, Dei MO. Reforming global criminal justice: Addressing corruption's impact on armed crime. Journal of Law and Legal Reform, 2024;5(3)1369-1404. https://doi.org/10.15294/jllr.v5i3.4082

15. Kniaziev SM, Smirnov A, Samokhvalova I, Tymoshenko Y, Morhunov O. Manipulation of sports competitions: Investigation and prevention. Pakistan Journal of Criminology, 2024;16(3):1111-1126. https://doi.org/10.62271/pjc.16.3.1111.1126

16. Kozachenko OI, Zarosylo VO, Gelemei MO, Stankovych MI, Yatsun MM. International cooperation in EU pre-trial investigations and its future role in Ukraine's legal reform. Journal of Law and Legal Reform, 2024;5(3):1405-1428. https://doi.org/10.15294/jllr.v5i3.3595

17. Ishchenko Y, Rusnak A, Artemov V, Syniavskyi P, Soroka I. Psychological and pedagogical aspects of adaptation of students who received temporary shelter to the educational environment of another country. Journal of Higher Education Theory and Practice, 2024;24(1). https://doi.org/10.33423/jhetp.v24i1.6766

18. Valyukevych TV, Zinchenko OZ, Ishchenko YO, Artemov V, Nechaiuk LG. Research-oriented framework of training philology students' research skills based on Corpus analytical software. European Journal of Educational Research, 2021;10(2):671-680. https://doi.org/10.12973/eu-jer.10.2.671

19. Equatora MA, Raja G. a/I, Anwar U, Saeed H, Hussain SM. Impact of terrorism on international trade in Pakistan. Journal of Mental Health and Social Rehabilitation, 2023;1(1):15–25. https://doi.org/10.52472/jmhsr.v1i1.198

20. DSG. Annex of statistical information 2022. [Internet]. 2023. Available from: https://www.state.gov/wp-content/uploads/2023/12/2022_Statistical_Annex_Final__508_Compliant-revised.pdf

21. Statista. Number of terrorist attacks worldwide between 2007 and 2022. Crime & Law Enforcement. [Internet]. 2023. Available from: https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/

22. Vision of Humanity. Overall terrorism index score. [Internte]. 2023. Available from: https://www.visionofhumanity.org/maps/global-terrorism-index/#/

23. Interpol. Interpol global crime trend summary report. [Internet]. 2022. Available from: https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

24. Sricharan K, Venkat M. Real-time drone detection using deep learning. In: Proceedings of the second international conference on emerging trends in engineering (ICETE 2023). Dordrecht: Atlantis Press International BV, 2023, pp. 905–918. https://doi.org/10.2991/978-94-6463-252-1_91

25. Mijalković S. Milašinović S. Methodological guidelines for the scientific research of false reports on planted explosive devices in the Republic of Serbia. Socioloski Pregled, 2023;57(4):1257–1278. https://doi.org/10.5937/socpreg57-48337

26. Green T. The problems and perils of muslims condemning terrorism. Journal of Muslim Philanthropy and Civil Society, 2023;7(1):4–20. https://doi.org/10.2979/jmpcs.7.1.01

27. Pettinger T. Embodying the inquiry: Disaster, affectivity, and the localized politics of security. Environment and Planning C: Politics and Space, 2023;41(7):1282–1300. https://doi.org/10.1177/23996544231195050

28. Ghalib, AM, Utama AP, Madjid MA, Widodo P. The role of the New Zealand government in handling terrorism through the media. International Journal of Humanities Education and Social Sciences (IJHESS), 2023;3(1). https://doi.org/10.55227/ijhess.v3i1.588

29. Shivdas S. Introduction to digital forensics. International Journal for Research in Applied Science and Engineering Technology, 2023;11(8):833–836. https://doi.org/10.22214/ijraset.2023.55258

30. Garciandía ID. The effectiveness of freedom of religion or belief as a framework in international relations: The case of Uyghur muslims and other religious minorities in Xinjiang, China. Review of Faith and International Affairs, 2023;21(2):95–106. https://doi.org/10.1080/15570274.2023.2200277

31. La Fors K, Meissner F. Contesting border artificial intelligence: Applying the guidance-ethics approach as a responsible design lens. Data and Policy, 2022;4(3). https://doi.org/10.1017/dap.2022.28

32. Malik AA, Azeem W, Asad M. The modern electronic and other technologies to combat new wave of terrorism and criminal activities. International Journal for Electronic Crime Investigation, 2023;7(3):8. https://doi.org/10.54692/ijeci.2023.0703156

33. Ahmed, Dimah A. Combating intellectual extremism and terrorism problems and challenges. Tikrit Journal For Political Science, 2023;3(pic4):614–630. https://doi.org/10.25130/tjfps.v3ipic4.250

34. Movchan A, Shliakhovskyi, O, Kozii V, Fedchak I. Investigating cryptocurrency financing crimes terrorism and armed aggression. Social and Legal Studios, 2023;6(4):123–131. https://doi.org/10.32518/sals4.2023.123

35. Patel VN. Terrorism – A universal problem. Research Journal of Humanities and Social Sciences, 2023:52–54. https://doi.org/10.52711/2321-5828.2023.00011

36. BENAMARA NK, Zigh E, Stambouli TB, Keche M. Towards a robust thermal-visible heterogeneous face recognition approach based on a cycle generative adversarial network. International Journal of Interactive Multimedia and Artificial Intelligence, 2022;7(4):132–145. https://doi.org/10.9781/ijimai.2021.12.003

FINANCING

None.

CONFLICT OF INTEREST

Authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Yevhen Bondarenko, Ivo Svoboda, Ivan Tkachov, Oleksandr Kozenko, Volodymyr Vislovukh.

Data curation: Yevhen Bondarenko, Ivo Svoboda, Ivan Tkachov, Oleksandr Kozenko, Volodymyr Vislovukh.

Formal analysis: Yevhen Bondarenko, Ivo Svoboda, Ivan Tkachov, Oleksandr Kozenko, Volodymyr Vislovukh.

Drafting - original draft: Yevhen Bondarenko, Ivo Svoboda, Ivan Tkachov, Oleksandr Kozenko, Volodymyr Vislovukh.

Writing - proofreading and editing: Yevhen Bondarenko, Ivo Svoboda, Ivan Tkachov, Oleksandr Kozenko, Volodymyr Vislovukh.