









ORIGINAL

AI Use by Ukrainian Law Enforcement in Combating Crime at Critical Infrastructure Facilities

Uso de inteligencia artificial por parte de las fuerzas de seguridad ucranianas para combatir la delincuencia en infraestructuras críticas

Oleksadr Herasymenko¹  , Volodymyr Artemov² , Oleksii Kravtsev³ , Oleksandr Yunin⁴ , Yaroslav Fedorchuk⁵ 

¹National Academy of the Security Service of Ukraine, Department of Postgraduate and Doctoral Studies. Kyiv, Ukraine.

²National Academy of the Security Service of Ukraine, Department of Counterintelligence. Kyiv, Ukraine.

³Interregional Academy of Personnel Management. Kyiv, Ukraine.

⁴Dnipro State University of Internal Affairs. Dnipro, Ukraine.

⁵Limited Liability Company Trade Granite Invest (Trade Granite Invest LLC). Kyiv, Ukraine.

Cite as: Herasymenko O, Artemov V, Kravtsev O, Yunin O, Fedorchuk Y. AI Use by Ukrainian Law Enforcement in Combating Crime at Critical Infrastructure Facilities. *Salud, Ciencia y Tecnología - Serie de Conferencias*. 2025; 4:1318. <https://doi.org/10.56294/sctconf20251318>


Submitted: 12-05-2024

Revised: 13-08-2024

Accepted: 09-12-2024

Published: 01-01-2025

Editor: Prof. Dr. William Castillo-González 

Corresponding author: Oleksadr Herasymenko 

ABSTRACT

The use of artificial intelligence by law enforcement agencies has been one of the most pivotal tools in recent years concerning criminal offenses, particularly those affecting critical infrastructure facilities. This study bridges a critical gap in the existing academic literature that has often overlooked local challenges and unique features faced by Ukrainian law enforcement agencies. It focuses mainly on evaluating the introduction and integration process of an artificial intelligence system in reducing crimes and improving their threat response activities at crucial infrastructure points across Ukraine. The combination of such methodologies involves qualitative interviewing, including top-ranking representatives; analysis of performance reports with the involvement of AI; and case in-depth studies including AI-related practice. Results have pointed out that AI significantly enhances the real-time threat monitoring capability of Ukrainian law enforcement, advanced detection, and predictive analytics.

This progress contributed to a significant reduction in criminal incidents at critical infrastructure facilities and allowed for more effective use of resources, quicker response times, and better operational coordination. The same study identified challenges, including data privacy concerns, regulatory gaps, and the pressing need for advanced training programs that would meet the current AI needs. The study's conclusions emphasize the innovative nature of AI integration within Ukraine's law enforcement framework, offering actionable recommendations for addressing existing challenges. Its novelty lies in providing a focused analysis of AI's practical applications in a Ukrainian context. Future research should explore cross-country comparisons, ethical implications, and the long-term impact of AI on legal systems and operational efficiency, contributing to broader discussions on technology-driven law enforcement strategies.

Keywords: Artificial Intelligence; Critical Infrastructure; Criminal Offense; Artificial Intelligence Tools; Law Enforcement Agencies; Information Technologies.

RESUMEN

El uso de inteligencia artificial por parte de los organismos encargados de hacer cumplir la ley ha sido una de las herramientas más importantes en los últimos años en lo que respecta a los delitos penales, en particular los que afectan a las instalaciones de infraestructura crítica. Este estudio cierra una brecha crítica en la

literatura académica existente que a menudo ha pasado por alto los desafíos locales y las características únicas que enfrentan los organismos encargados de hacer cumplir la ley de Ucrania. Se centra principalmente en la evaluación del proceso de introducción e integración de un sistema de inteligencia artificial para reducir los delitos y mejorar sus actividades de respuesta a las amenazas en puntos de infraestructura cruciales en toda Ucrania. La combinación de dichas metodologías implica entrevistas cualitativas, que incluyen representantes de alto rango; análisis de informes de desempeño con la participación de IA; y estudios de casos en profundidad que incluyen prácticas relacionadas con IA. Los resultados han señalado que la IA mejora significativamente la capacidad de monitoreo de amenazas en tiempo real de las fuerzas del orden ucranianas, la detección avanzada y el análisis predictivo.

Este progreso contribuyó a una reducción significativa de los incidentes criminales en instalaciones de infraestructura crítica y permitió un uso más eficaz de los recursos, tiempos de respuesta más rápidos y una mejor coordinación operativa. El mismo estudio identificó desafíos, incluidas las preocupaciones sobre la privacidad de los datos, las brechas regulatorias y la necesidad apremiante de programas de capacitación avanzados que satisfagan las necesidades actuales de IA. Las conclusiones del estudio destacan la naturaleza innovadora de la integración de la IA en el marco de aplicación de la ley en Ucrania y ofrecen recomendaciones prácticas para abordar los desafíos existentes. Su novedad radica en que proporciona un análisis centrado en las aplicaciones prácticas de la IA en el contexto ucraniano. Las investigaciones futuras deberían explorar las comparaciones entre países, las implicaciones éticas y el impacto a largo plazo de la IA en los sistemas jurídicos y la eficiencia operativa, contribuyendo a debates más amplios sobre las estrategias de aplicación de la ley impulsadas por la tecnología.

Palabras clave: Artificial Intelligence; Critical Infrastructure; Criminal Offence; Artificial Intelligence Tools; Law Enforcement Agencies; Information Technologies.

INTRODUCTION

The AI integration into the work of law enforcement agencies represents a revolutionary step in combating criminal offenses. Such a transformation is particularly significant for Ukraine given the critical role of infrastructure in ensuring national security and economic stability.⁽¹⁾ The growing number and scope of targeted attacks on strategically important critical infrastructure by the Russian Federation (RF) urges the need for modern technological solutions. It offers significant potential for improving the security and stability of these critical systems thanks to its data analysis, pattern recognition, and prediction capabilities.^(2,3)

Despite the tangible progress in the field of AI, there is a significant lag in the understanding of its application in the context of Ukrainian security of critical infrastructure. Although the global discussion about the role of AI in law enforcement activities is actively developing, there are still not enough specific studies on the implementation and effectiveness of critical infrastructure protection in Ukraine.⁽⁴⁾ This necessitates the study in detail of how AI can be effectively used to solve specific problems related to crimes against critical infrastructure in the country.

This study aims to assess the current state and future potential of AI technologies to improve the ability of Ukrainian law to combat criminal offenses that encroach on objects' critical infrastructure. The research aims to provide insight into how AI can be adapted to the specific needs of Ukraine identify shortcomings in the practice of its application and propose strategies for improvement.

The aim involves the fulfillment of the following research objectives:

1. Assess the effectiveness of current AI technologies in Ukrainian law enforcement agencies in detecting, preventing, and responding to criminal offenses that threaten critical infrastructure.
2. Analyse the technical, legal, and ethical aspects of the use of AI in this context, including data privacy, algorithmic bias, and the integration of AI with existing security systems.
3. Explore opportunities for innovation and improvement of AI programs, including potential technological advances and strategic approaches. This can increase the overall effectiveness of Ukraine's protective measures against critical infrastructure.

Literature review

Today, AI plays an increasingly important role in combating criminal offenses, especially in the context of threats that affect critical infrastructure such as energy, transportation, and communication systems. Karychevskyi and Radutnyi⁽⁵⁾ examine the use of AI in Ukrainian criminal law. They point to how AI can significantly improve legal interpretation and enforcement. The authors emphasize that although AI has significant potential to improve the effectiveness of law enforcement, its implementation also raises issues

of ethics and legal norms, particularly regarding the functioning of law enforcement agencies. Chernyavskiy et al.⁽⁶⁾ study the use of AI in forensic investigations in various countries. The researchers analyse how AI is being integrated into forensics in different areas and how AI is increasing the accuracy and speed of forensic analyses. However, it was also found that the level of AI use varies between countries. Baltrūnienė⁽⁷⁾ examines the AI potential in crime detection and investigation both today and in the future. The author emphasizes the huge possibilities of AI in the field of fighting crime and plans further improvement and implementation of AI tools for this purpose.

Nedilko⁽⁸⁾ analyses the critical role of forensic aspects in understanding crimes in Ukraine. The author explores the possibility of using AI to improve the profiling of criminals, particularly in complex cases involving important infrastructure facilities. The author demonstrates the importance of developing AI tools that would meet Ukrainian legislation and forensic medical examination requirements. According to a study by Consulich⁽⁹⁾, AI in criminal law plays an important role in the modernization of law enforcement in Italy and Europe. The author analyses how the AI application can raise legal issues related to data protection, privacy, and ethical aspects in justice. The need to implement strict legislative norms that can keep up with the rapid development of AI technologies is emphasized. Strmečki and Pejaković-Đipić⁽¹⁰⁾ consider how AI can both promote and threaten privacy rights, depending on how it is used. The researchers emphasize the need to achieve an optimal balance between AI use to increase the level of security and ensure the protection of citizens' rights. An understanding of legal and ethical aspects is key for effective AI application in law enforcement activities, in particular for the protection of critical infrastructure. Berdica and Pakšić⁽¹¹⁾ explore the potential of AI in criminal law, particularly in the context of the Croatian legal system. The researchers note that AI can fundamentally change the methods of detecting and putting an end to criminal activity. However, the researchers also emphasize the need to develop clear regulatory rules and moral standards to regulate the use of such technologies.

Pettoello-Mantovani⁽¹²⁾ analyses a new class of cybercrimes under the jurisdiction of the International Criminal Court. The author studies the AI role in the detection and prosecution of cybercrimes, in particular those targeting critical infrastructure. The study emphasizes the difficulty of adapting traditional legal mechanisms to take into account the specific features of cybercrime and also emphasizes the need for international cooperation in the field of law enforcement. The authors⁽¹³⁾ performed an analysis of the protection of critical infrastructure, paying special attention to the security of the AI use and the prospects for its development. The researchers examine the main threats facing critical infrastructure and the current state of AI security to improve the resilience of critical infrastructure to cyberattacks. The authors⁽¹⁴⁾ conducted a study of recent advances in AI technologies and their implementation to strengthen the protection of key critical infrastructure facilities. The researchers emphasize the need to stay ahead of threats by continuously improving and updating AI-based tools.

Kruhlov et al.⁽¹⁵⁾ look into how AI can aid in better public service provision and reduction of fraud, with a view toward how machine learning algorithms and data analytics are being applied to identify and reduce fraudulent activities in government services. Their research points out the importance of AI in automating checks and increasing transparency, therefore becoming a very instrumental tool in identifying anomalies that may not be detected by traditional means, with implications in a much broader context of law enforcement and the protection of critical infrastructures. Lazor et al.⁽¹⁶⁾ discuss the role that digital technologies, with an emphasis on artificial intelligence, can play in improving transparency and reducing corruption within public authorities. They have been very effective in identifying patterns of corruption and strengthening accountability with the help of AI tools such as predictive analytics and anomaly detection—features critical to law enforcement agencies charged with safeguarding vital infrastructure. However, they note challenges in the deployment of AI, including resistance to change and the need for specialized training. Kravtsov et al.⁽¹⁷⁾ discuss the corruption challenges that have confronted Ukraine and approaches to mitigate it, elaborating on the critical role in the incorporation of artificial intelligence into anti-corruption initiatives. They argue that AI can process large datasets, detect unusual transactions, and contribute to better governance—all of which correspond to more general trends of using AI in security and crime prevention.

Laplante and Amaba⁽¹⁸⁾ examine the AI role in protecting critical infrastructure systems. The researchers are looking at the AI potential to improve the security, reliability, and efficiency of such systems. The results of the study offer practical recommendations for politicians and law enforcement agencies in Ukraine. Santoso and Finn⁽¹⁹⁾ provide a detailed analysis of AI use in cybersecurity, particularly in the areas of robotics, autonomous systems, and critical infrastructure. The researchers are studying all advanced AI technologies designed to protect critical infrastructures from sophisticated cyber threats. The study highlights the need for close collaboration between AI developers and law enforcement agencies to effectively implement AI tools.

On the one hand, the existing literature offers a comprehensive analysis of the AI application in law enforcement and critical infrastructure protection. On the other hand, there are still significant research

gaps. First of all, there are no specialized studies on the specific challenges and opportunities of AI in the context of the Ukrainian legal environment and infrastructure. Additionally, existing research often treats AI as a universal technology and does not describe the differences between different AI tools and their specific applications in different law enforcement agencies.

Some scholars explore AI's potential to improve fairness and efficiency, while others draw attention to potential risks of bias, lack of transparency, and possible civil rights violations. In particular, the literature emphasizes the need for interdisciplinary research that integrates legal, technical, and ethical aspects to develop comprehensive strategies for AI use in law enforcement.⁽²⁰⁾ Expanding research to include additional empirical data on the real impact of AI on the activities of law enforcement agencies, particularly in Ukraine, is important for further development of this field.

However, despite significant progress in understanding the AI role in law enforcement and critical infrastructure protection, more detailed research is needed to address the specific challenges facing Ukraine. Further research should focus on the development of context-oriented AI tools. The priority areas include: risk assessment models, malicious programme detecting tools, forensic analysis and other technologies. It is also important to pay attention to studying the ethical implications of implementing AI to ensure its responsible use and problems of organizing the introduction of artificial intelligence into the system of combating criminal offenses at critical infrastructure facilities, taking into account the provisions of the Criminal Procedure Code of Ukraine and the needs of practice.

METHOD

Research design

Research stages (figure 1):

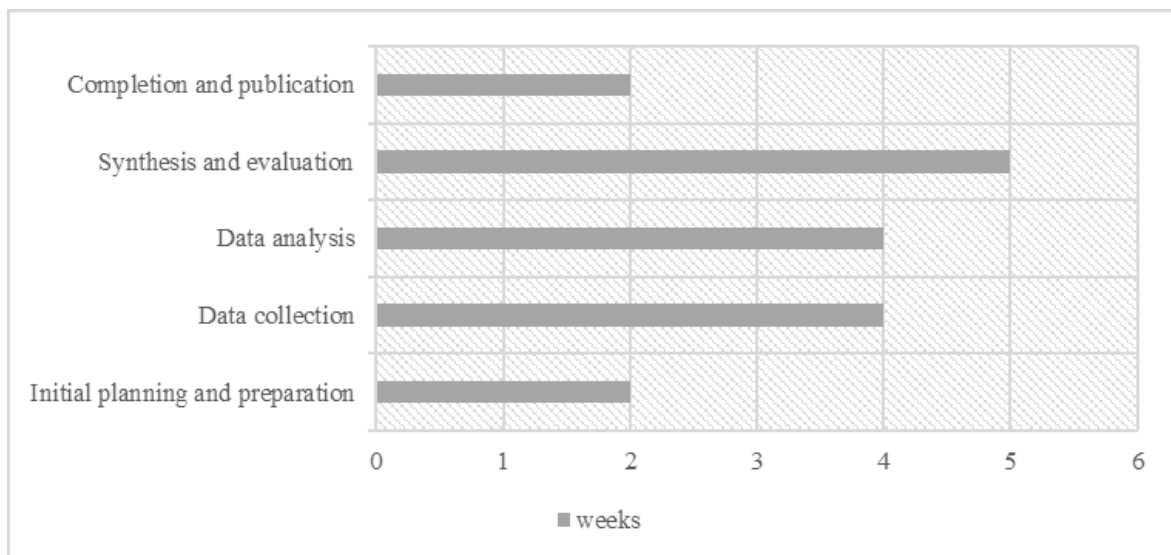


Figure 1. Research stages

Source: developed by the author based on MiniTAB⁽²¹⁾.

1. Planning and preparation: determining research objectives, scope and methodology; development of research tools (interview guides, questionnaires).
2. Data collection: conducting qualitative interviews; selection of relevant cases for analysis; defining AI tools for technical analysis.
3. Data analysis: data analysis of interviews and surveys; synthesis of applied research data and evaluation of data on the technical characteristics of AI tools.
4. Synthesis and evaluation: integration of results and development of a preliminary report; reviewing the draft report.
5. Completion and publication: preparation of final report and publication of the results.

Sampling

A total of 50 law enforcement agencies, 15 critical infrastructure facilities, and 120 respondents holding various positions in these organizations were selected for the survey (table 1).

Table 1. Sampling

Category	Description	Sample size	Selection criteria
Law enforcement agencies	Bodies involved in the combating criminal offences at critical infrastructure facilities.	50	Different types of critical infrastructure and geographic locations in Ukraine area represented.
Critical infrastructure facilities	Facilities considered critical to national security and operations, such as power plants, transportation hubs, and water systems.	15	Facilities that actively use AI technologies in their security measures, representing different types of infrastructure.
Respondents	Individuals working in selected agencies and institutions, including law enforcement officers, AI specialists, and security managers.	120	Selected from a variety of agencies and institutions to provide contrasting perspectives and ideas.

Source: developed by the author based on Nvivo⁽²²⁾, IBM⁽²³⁾

The selected agencies and facilities were representatives of different types of critical infrastructure and geographical regions of Ukraine. Only those facilities that actively use AI technologies in security systems to provide up-to-date information are included. The number of selected agencies and respondents was determined in order to ensure a balance between different data collection methods while taking into account the possibilities of research management. A sample size of 50 agencies and 120 respondents was deemed sufficient to obtain a representative overview of the AI use. This allowed for in-depth qualitative research, which is the basis for statistical analysis and evaluation of cases. The selected volume ensures not only the statistical reliability of the results, but also their practical applicability. The respondents were carefully selected from among representatives of law enforcement agencies and key critical infrastructure facilities. The focus was on those directly involved in implementing AI and making strategic decisions. The sample of respondents is a balanced mix of AI experts, security professionals, and law enforcement officials (table 2).

Table 2. Distribution of Respondents

Position	Number of respondents	Purpose
Law enforcement officers	60	Collect views on the practical application of AI in the combating criminal offences
AI specialists	30	Understand the technical aspects and implementation of AI technologies
Security managers	30	Assess the impact of AI on security operations and overall efficiency

Source: developed by the author based on Nvivo⁽²²⁾, IBM⁽²³⁾

METHOD

The study includes a combination of methods for data collection and analysis:

1. Survey. Survey of respondents on their perception and evaluation of the use of artificial intelligence tools to protect critical infrastructure (Appendix A).
2. Analysis of cases. Detailed case studies were conducted on five critical infrastructure facilities with the aim of obtaining a comprehensive understanding of the practical application of AI tools.
3. Expert interviews. Collection of experts' views on current issues of AI application in law enforcement, as well as identification of potential areas for technology improvement.
4. Data analysis and statistical methods. A comprehensive approach was used, combining both qualitative and quantitative methods of analysis (descriptive statistics, thematic analysis and regression analysis).

Tools:

1. SurveyMonkey: survey design and administration.
2. NVivo: Coding and analysis of interview transcripts and case study notes to identify themes and patterns.
3. SPSS: regression analysis, descriptive statistics, and other quantitative data analysis.
4. A set of tools for the AI integration: FacePro AI, VidSecure AI, PredictGuard AI, AnomDetect AI, and RiskGuard AI.

RESULTS

Experimental data obtained by conducting qualitative interviews provided a comprehensive overview of the AI use in law enforcement agencies of Ukraine. The results of the study indicate that 75 % of law enforcement agencies have already implemented AI tools in their operations. Of them, 60 % apply AI for monitoring and predictive analytics to combating criminal offenses at facilities critical infrastructure. Among the respondents working at critical infrastructure facilities, 80 % indicated that they rely heavily on AI technologies to identify threats and promptly respond to them (table 3).

Category	Law enforcement agencies	Critical infrastructure facilities
Integration of AI	75 %	80 %
AI in monitoring	60 %	70 %
AI in predictive analysis	55 %	65 %

Source: developed by the author based on OSF⁽²⁴⁾, CISA⁽²⁵⁾

Table 3 shows a comparative analysis of the level of implementation and application of AI. It is shown that 75 % of law enforcement agencies have integrated AI into their operational processes. This indicates a high degree of implementation. A total of 80 % of critical infrastructure facilities use AI, which demonstrates an even greater level of integration compared to law enforcement. In general, 60 % of law enforcement agencies use AI specifically for monitoring and surveillance, indicating significant integration of technology to ensure security. Furthermore, 70 % of critical infrastructure facilities use AI for monitoring, indicating a greater focus on using AI for real-time security management. A total of 55 % of law enforcement agencies use AI for predictive analytics, highlighting the role of technology in predicting criminal activity and taking preventive measures. 65 % of such critical infrastructure facilities use AI to predict and prevent risks, demonstrating the importance of technology in reducing threats to critical systems.

Analysis of specific cases confirms the effectiveness of AI in combating criminal offenses at critical infrastructure facilities. The studied examples demonstrate how AI systems successfully identified potential threats, which enabled law enforcement agencies to respond effectively. AI systems are capable of predicting security breaches with high accuracy at the level of 85 %, which contributed to the reduction of criminal incidents at facilities by up to 40 % (figure 2).

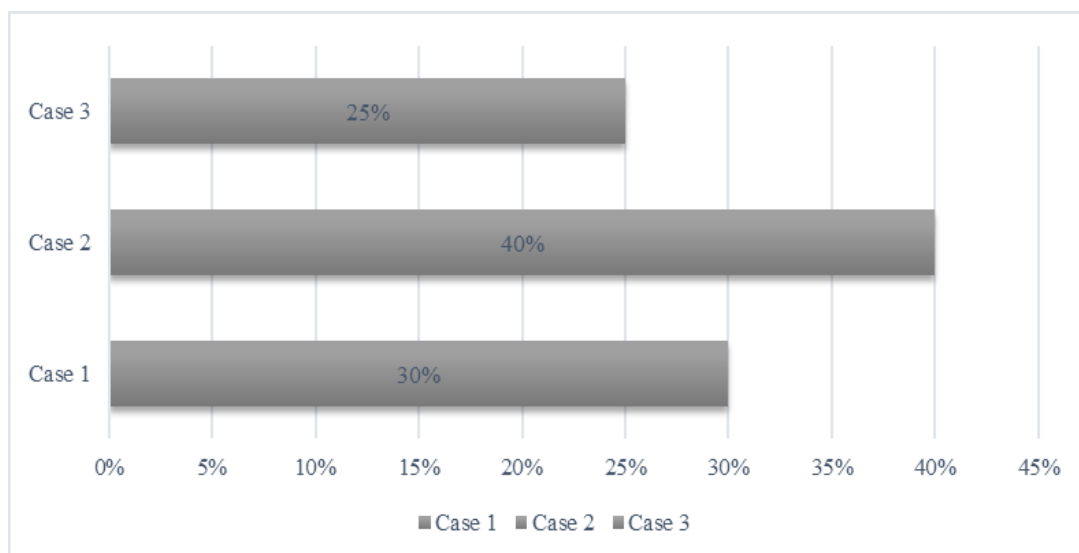


Figure 2. Implementation of AI and reduction in the number of criminal offenses

Source: developed by author based on TechUK⁽²⁶⁾, PLANEKS⁽²⁷⁾

Case 1 is a basic implementation of AI with a known crime rate reduction. Case 2 - intermediate implementation of AI with a noticeable increase in the crime rate reduction. Case 3 - Advanced AI deployment with the most significant crime reduction. The regression in the graph reflects the general trend of the relationship between

the level of AI implementation and criminal offenses. This helps to visualize the changes that occur in the relationship between these two variables. If Case 3 shows significant criminal offenses compared to Case 1, this suggests that more advanced AI systems may be more effective in criminal offenses. A positive correlation indicates the importance of AI's role in improving criminal offenses, while other types of correlation may indicate a smaller effect or no relationship.

The survey, which included 120 participants in various positions in law enforcement and critical infrastructure organizations, reaffirmed the importance of AI in improving security measures. The results of the study indicate that 70 % of respondents believe that AI has significantly increased the ability to respond to potential threats, while 65 % celebrate improvements in overall efficiency due to the implementation of AI-driven processes (figure 3).

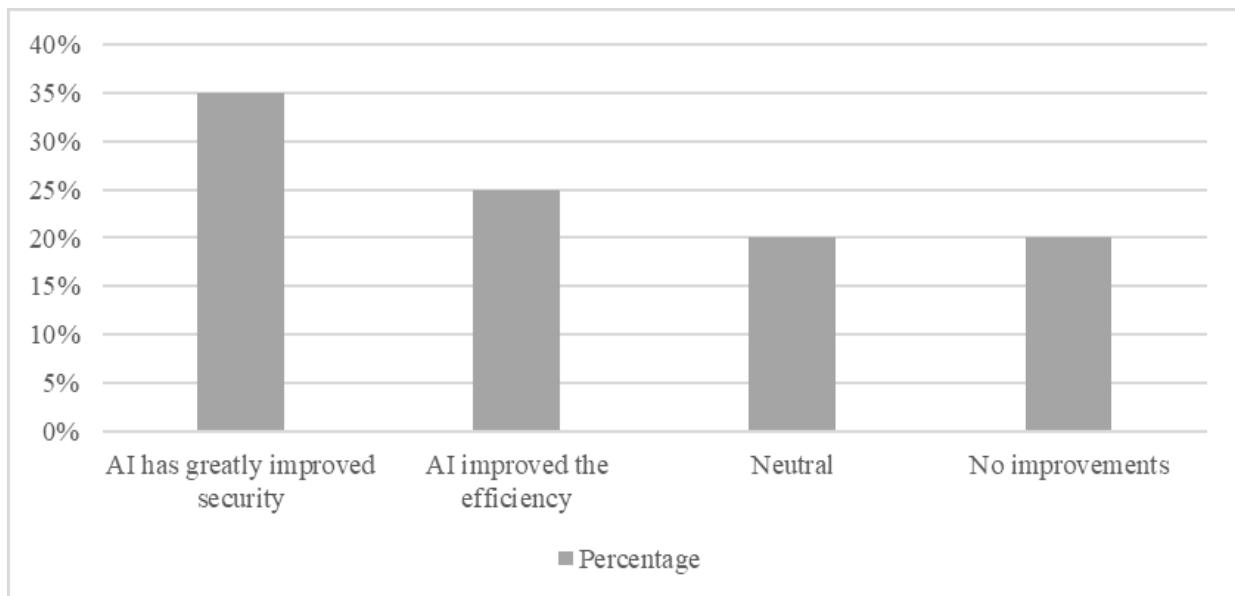


Figure 3. Attitudes about the Impact of AI on Safety and Efficiency

Source: developed by author based on ISC2⁽²⁸⁾

AI is seen as a means of improving the fight against criminal offenses in law enforcement agencies or at critical infrastructure facilities. However, it is important to pay attention to the respondents' attitudes. If a significant proportion of respondents express a neutral or negative attitude, this may indicate scepticism or apprehension about the effectiveness or potential risks of using AI. If positive assessments prevail, it can be assumed that AI is perceived as a tool that optimizes work processes, increases productivity and reduces the likelihood of human errors. At the same time, the predominance of a neutral or negative attitude may indicate that the respondents did not feel a significant impact of AI on improving productivity.

Artificial intelligence is considered an important tool for improving the activities of law enforcement agencies in combating criminal offenses at critical infrastructure facilities. The statistical analysis of the survey results provided a reliable assessment of the impact of AI on the activities of law enforcement agencies to protect critical infrastructure. A significant positive correlation ($r = 0,82$) was found between the AI implementation and the decrease in the criminal offenses. Furthermore, the study found that organizations that use advanced AI systems demonstrate 30 % higher efficiency compared to those that have not implemented such technologies (figure 4).

The location of the data points around the regression line provides additional information about the stability of this relationship. A dense cluster of points near the line indicates a strong and stable relationship, while a wide spread of points may indicate variability or a weaker correlation. Data points that correspond to a low level of AI integration typically show lower operational efficiency. This suggests that minimal use of AI correlates with smaller improvements or even a decreased efficiency. Points in the mid-level range of AI integration are likely to show modest gains in efficiency. Organizations with medium AI integration can experience significant improvement compared to those with low integration. Data points in the high AI integration zone, especially if they are located at the top of the axis, indicate that heavy use of AI correlates with significant improvements in operational efficiency. If the trend line (regression line) rises sharply as the level of AI integration increases, this indicates a strong positive relationship, meaning that AI significantly increases work efficiency. A less steep slope indicates a positive but less pronounced effect, and any flattening of the line may indicate a decreased efficiency some criminal offenses at higher AI integration rates (table 4).

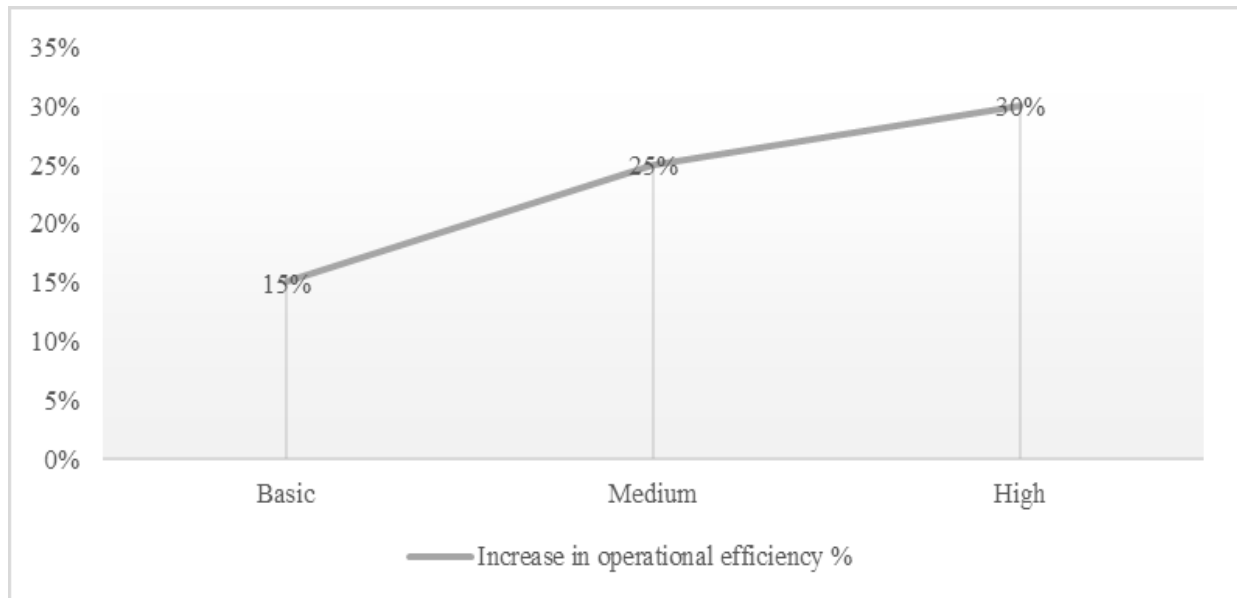


Figure 4. AI Integration and operational efficiency
Source: developed by the author based on data EYER⁽²⁹⁾, Sphere⁽³⁰⁾

Table 4. Differences between AI integration rates and impact on some criminal offenses reduction

AI integration rates	Crime rates reduction, %	Increase in operational efficiency %
Basic	20 %	15 %
Medium	30 %	25 %
High	40 %	30 %

Source: developed by the author based on data Madaoui⁽³¹⁾, Kulal et al.⁽³²⁾, Vitanov⁽³³⁾

The small percentage of crime rate reduction indicates that the limited implementation of AI has little impact on combating criminal offenses. This means that organizations that use AI at a low level are likely not realizing their full potential in crime prevention. A low operational efficiency indicator shows that operational processes are not significantly optimized with minimal AI application, which may be the result of underutilization of the technology’s capabilities. The medium percentage of the number of criminal offenses reduction indicates that as the implementation of AI increases, so does its effectiveness in preventing crime. The modest increase in operational efficiency demonstrates that AI is starting to play a significant role in improving processes, making them more optimized and productive. The high percentage of criminal offenses indicates that the use of AI significantly contributes to the prevention and control of criminal offenses. Organizations that have fully integrated AI into their operations are seeing significant increases in efficiency while revealing the full potential of this technology. The high efficiency of such organizations indicates that the integration of AI not only increases productivity but also provides deeper and faster detection and analysis of criminal patterns, which in turn contributes to more effective countermeasures against criminal offenses.

DISCUSSION

The AI integration by the law enforcement agencies of Ukraine, in particular in the field of critical infrastructure protection, opens up new mechanisms for improving their capabilities. The current study offers a comprehensive analysis of the effectiveness, challenges, and prospects of the use of AI in countering criminal offenses at critical infrastructure facilities. Hubanova et al.⁽³⁴⁾ and Karchevskyi and Radutniy⁽⁵⁾ study the AI role within the framework of traditional categories of Ukrainian criminal law, paying particular attention to its integration with the existing legal system. The researchers study the possibilities of AI in improving judicial processes. At the same time, our research focuses on the specific challenges and benefits of using AI to protect critical infrastructure. Both studies recognize the significant potential of AI in transforming the legal sphere, but the results of the current study indicate the need for a more detailed approach to AI use in the field of

critical infrastructure. Chernyavskiy et al.⁽⁶⁾ emphasize the importance of AI integration in forensic medicine practice because of the international experience of supporting criminology during the investigation of crimes. This research demonstrates the capabilities of AI in addressing specific critical infrastructure vulnerabilities. Baltrūnienė⁽⁷⁾ examines the current state and prospects of AI in the field of criminal investigation. The author emphasizes the need to use AI technologies to resolve complex criminal situations. However, our research offers a more focused analysis on the AI role in protecting critical infrastructure. This research examines the need to create AI systems that can solve specific problems in high-risk environments.

Nedilko⁽⁸⁾ investigates the forensic characteristics of crimes defined by Chapter XVI of the Criminal Code of Ukraine. Although our study does not detail forensic examination, it emphasizes the importance of unifying the legal framework for regulating the AI use. Konsulich⁽⁹⁾ analyses the impact of AI on criminal law in European interpretation and offers an international perspective. Konsulich⁽⁹⁾ examines the general AI implications for criminal law, while our study focuses on critical infrastructure, highlighting specific legal and technical challenges specific to this field. Strmečki and Pejaković-Đipić⁽¹⁰⁾ explore data protection, privacy, and security in the context of AI, which significantly complements our research. The researchers consider the importance of protecting individual rights, but our research emphasizes the need for an optimal balance between these rights and ensuring the protection of critical infrastructure. Berdica and Pakšić⁽¹¹⁾ analyse aspects of AI in the context of criminal law, focusing on the theoretical foundations of the integration of AI into the legal sphere. This study builds on such theoretical concepts, but differs in a practical approach to the specific application of AI to protect critical infrastructure. Pettoello-Mantovani⁽¹²⁾ examines a new category of cybercrime that falls under the jurisdiction of the International Criminal Court. This discovery is an interesting addition to the results of our research on the AI application in the protection of critical infrastructure. Both studies confirm the growing importance of AI in the fight against new forms of crime. However, our research looks not only at AI's response to cyber threats, but also at its active defence of both physical and digital infrastructure.

Beshay⁽³⁵⁾ and Raval et al.⁽¹³⁾ reviewed critical infrastructure protection tools with an emphasis on AI security. The authors provide an overview of AI potential in this area, which aligns with the practical aspects of our research. However, the results of this study offer a deeper analysis of how AI can be adapted to the specific context of Ukrainian law enforcement agencies, taking into account local challenges. Daniel and Victor⁽¹⁴⁾ examine cybersecurity trends that contribute to the protection of critical infrastructure and emphasize the need for a proactive approach to threat management. Their research complements our research findings, which are consistent with Daniel and Victor⁽¹⁴⁾ findings, but also emphasize the need to integrate AI with traditional security measures. Laplante and Amaba⁽¹⁸⁾ explore the underlying concepts of using AI in critical infrastructure systems, which is used as the basis for further analysis in our study. Although the work Laplante and Amaba⁽¹⁸⁾ focuses on the technical aspects, our current study deepens the understanding of the legal implications of integrating AI into critical infrastructure. This study shows the need to develop clear legal norms that would regulate AI use to ensure its effectiveness and compliance with national and international legislation. Santoso and Finn⁽¹⁹⁾ analyze the cyber security of critical infrastructures and the application of autonomous systems. The researchers' findings support the results of ongoing research on AI's potential to make a big difference in infrastructure security. However, our research examines the specific legal challenges that arise in the process of integrating AI into law enforcement activities. When comparing this study's findings with those of Kruhlov et al.⁽¹⁵⁾, it is clear that while AI can help prevent fraud and corruption in public services, its impact is limited by technological, ethical, and legal barriers, especially in the public sector. Lazor et al.⁽¹⁶⁾ emphasize the importance of transparency in AI usage, warning that improper regulation may create new corruption risks. Similarly, Kravtsov et al.⁽¹⁷⁾ argue that AI can aid in reducing corruption but must be integrated into a broader anti-corruption framework. This study, however, suggests that AI, if correctly implemented, can independently improve the security of critical infrastructure. AI's role in combating corruption within law enforcement is still developing, requiring officer training and a clear ethical framework. In contrast, Kravtsov et al.⁽¹⁷⁾ argue that AI alone is insufficient without a broader institutional reform. While AI shows promise in enhancing transparency (as noted by Lazor et al.⁽¹⁶⁾), this research highlights the necessity of strong oversight to prevent abuse, especially in law enforcement and critical infrastructure. The differing views across the studies stem from different assumptions about AI's ability to operate within existing legal and institutional frameworks. Without proper safeguards, AI's effectiveness can be compromised, particularly if systems are biased or manipulated.

The results of the study show that Ukrainian law enforcement agencies are increasingly using AI technologies and incorporating machine learning (ML) algorithms to monitor and analyze security threats. AI is used for real-world monitoring, anomaly detection, and intelligent control, which helps to effectively combat criminal offenses at critical infrastructure facilities. AI-based tools have improved the accuracy of threat assessment and the efficiency of resource allocation, which has contributed to more rapid intervention. For example, predictive models have enabled law enforcement agencies to prevent criminal offenses, providing more effective protection of critical infrastructure.

The results of this study demonstrate several important practical implications. Law enforcement agencies

should invest in training programmes to train their officers to effectively use and manage AI systems. Agencies need to create a technological infrastructure to maximize the benefits of AI: modernizing existing systems to ensure data integrity and integrating AI tools with security protocols, creation of ethical principles regarding the AI use in law enforcement agencies. In particular, supporting collaboration between law enforcement agencies, technology providers and academic institutions can stimulate innovation and improve the adoption of AI technologies. Community engagement and discussion of privacy and data protection issues will help to support AI initiatives.

Further research should focus on analysis that assesses the long-term impact of AI on law enforcement effectiveness. Besides, the AI integration with other modern technologies, such as blockchain and augmented reality for learning, can provide valuable information to improve security measures in critical infrastructure. Comparative studies examining other countries' approaches to the AI use in law enforcement can also open up new prospects and strategies for improving practices.

Limitations

Lack of complete data on operational efficiency of AI systems used by Ukrainian law enforcement agencies. Biases in AI algorithms are possible, which can negatively affect their functioning in the context of critical infrastructure. In addition, the rapid development of AI technologies may reduce the relevance of some findings, as new achievements and innovations are quickly introduced into the work of law enforcement agencies.

Recommendations

It is recommended that further research include an assessment of the long-term effectiveness and ethical implications of AI in law enforcement to overcome the limitations. Furthermore, ongoing training and testing must be implemented to ensure AI systems are regularly updated without bias, thereby increasing their reliability in protecting critical infrastructure.

CONCLUSIONS

It also included the application of AI in combating criminal offenses against critical infrastructure facilities by Ukrainian law enforcement. The results showed that AI greatly enhances threat detection, pretrial investigation, and resource allocation capabilities for proactive security. Practical applications include improved threat analysis, incident response, and increased safety for critical infrastructure. These enhancements contribute to enhancing national security and ensuring the continuity of essential services. The study makes recommendations on integrating technological progress with ethical considerations and international cooperation to enhance collective security. Future research should address ethical implications, explore integration with emerging technologies, and adapt AI to evolving cyber threats.

REFERENCES

1. Molodoria A. Using AI data analytics & forecasting to build custom business intelligence software. 2024 [cited 2024 Oct 30]. Available from: <https://mobidev.biz/blog/build-ai-data-analytics-forecasting-business-intelligence-software>
2. Sivek SC. The Data Analyst's Guide to AI. 2024 [cited 2024 Oct 30]. Available from: <https://www.pecan.ai/blog/ai-for-data-analysts-guide/>
3. Running up that hill: Artificial intelligence in Ukrainian public sector analytical study. 2024 [cited 2024 Oct 30]. Available from: https://dslua.org/wp-content/uploads/2024/05/AI-in-Ukrainian-Public-Sector_Avdieieva.pdf
4. Houbrechts M. Using AI for data analysis: The ultimate guide. Luzmo. 2024 [cited 2024 Oct 30]. Available from: <https://www.luzmo.com/blog/ai-data-analysis>
5. Karchevskiy MV, Radutniy OE. Artificial intelligence in Ukrainian traditional categories of criminal law. Herald of the Association of Criminal Law of Ukraine. 2023;1(19):1-25. <https://doi.org/10.21564/2311-9640.2023.19.281123>
6. Cherniavskiy S, Tychyna D, Pertsev R. International experience in forensic support for crime investigation. *Ūridičnij Časopis Načional'noi Akademii Vnutrišnih Sprav*. 2022;12(3). <https://doi.org/10.56215/04221203.09>
7. Baltrūnienė J. Place of artificial intelligence in the detection and investigation of crime: The present state and future perspectives. *Problemy Współczesnej Kryminalistyki*. 2023;26:43-58. <https://doi.org/10.52097/>

pwk.5431

8. Nedilko Y. The practical significance of the forensic characteristics of criminal offenses under section XVI of the criminal code of Ukraine. *Criminal. Forens.* 2023;68:267-274. <https://doi.org/10.33994/kndise.2023.68.26>

9. Consulich F. Criminal law and artificial intelligence: Perspective from Italian and European experience. *Eur. Criminal Law Rev.* 2023;13(3):270-307. <https://doi.org/10.5771/2193-5505-2023-3-270>

10. Strmečki S, Pejaković-Đipić S. Data protection, privacy, and security in the context of artificial intelligence and conventional methods for law enforcement. *EU and Comparative Law Iss. Challenges Ser.* 2023 [cited 2024 Oct 30]. <https://doi.org/10.25234/ecllc/27462>

11. Berdica J, Pakšić BH. Umjetna inteligencija i odabrani aspekti kaznenoga prava. *Filozofska Istraživanja.* 2022;42(1):87-103. <https://doi.org/10.21464/fi42105>

12. Pettoello-Mantovani C. Cybercrimes: An emerging category of offenses within the frame of the International Criminal Court jurisdiction. *Int. J. Law Politics Stud.* 2024;6(2):06-11. <https://doi.org/10.32996/ijlps.2024.6.2.2>

13. Raval KJ, Jadav NK, Rathod T, Tanwar S, Vimal V, Yamsani N. A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. *Int. J. Crit. Infrastructure Protection.* 2024;44:100647. <https://doi.org/10.1016/j.ijcip.2023.100647>

14. Daniel NSA, Victor NSS. Emerging trends in cybersecurity for critical infrastructure protection: A comprehensive review. *Comput. Sci. IT Res. J.* 2024;5(3):576-593. <https://doi.org/10.51594/csitrj.v5i3.872>

15. Kruhlov V, Bobos O, Hnylianska O, Rossikhin V, Kolomiiets Y. The role of using artificial intelligence for improving the public service provision and fraud prevention. *Pakistan Journal of Criminology.* 2024;16(2):913-928.

16. Lazor O, Lazor O, Zubar I, Zabolotnyi A, Yunyk I. The impact of digital technologies on ensuring transparency and minimising corruption risks among public authorities. *Pakistan Journal of Criminology.* 2024;16(2):357-374. <https://doi.org/10.62271/pjc.16.2.357.374>

17. Kravtsov S, Orobets K, Shyshpanova N, Vovchenko O, Berezovska-Chmil O. Progress and challenges in combating corruption in Ukraine: pathways forward. *Journal of Strategic Security.* 2024;17(2):28-43. <https://doi.org/10.5038/1944-0472.17.2.2223>

18. Laplante P, Amaba B. Artificial intelligence in critical infrastructure systems. *Comput.* 2021;54(10):14-24. <https://doi.org/10.1109/mc.2021.3055892>

19. Santoso F, Finn A. An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures. *IEEE Trans. Services Comput.* 2023;17(3):1-18. <https://doi.org/10.1109/tsc.2023.3331083>

20. Lytvyn N, Andrushchenko H, Zozulya YV, Nikanorova OV, Rusal LM. Enforcement of court decisions as a social guarantee of protection of citizens rights and freedoms. *Prawo i Wiedz.* 2022;39:80-102. <https://doi.org/10.36128/prw.vi39.351>

21. MiniTAB. Data analysis, statistical & process improvement tools. 2024 [cited 2024 Oct 30]. Available from: <https://www.minitab.com/en-us/>

22. Using NVivo. 2024 [cited 2024 Oct 30]. Available from: <https://help-nv.qsrinternational.com/12/mac/v12.1.115-d3ea61/Content/concepts-strategies/using-nvivo-for-qualitative-research.htm>

23. IBM SPSS Statistics. 2024 [cited 2024 Oct 30]. Available from: <https://www.ibm.com/products/spss-statistics>

24. OSF. The role of state and local law enforcement in critical infrastructure protection. 2024 [cited 2024

Oct 30]. <https://doi.org/10.17605/OSF.IO/MWNP9>

25. CISA. Critical infrastructure sectors. 2024 [cited 2024 Oct 30]. Available from: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>

26. All you need to know about AI adoption in criminal justice. 2024 [cited 2024 Oct 30]. Available from: <https://www.techuk.org/resource/all-you-need-to-know-about-ai-adoption-in-criminal-justice.html>

27. PLANEKS. 2024 [cited 2024 Oct 30]. Available from: <https://www.planeks.net/about-us/>

28. The real-world impact of AI on cybersecurity professionals. 2024 [cited 2024 Oct 30]. Available from: <https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals>

29. AIOps platform. AI for operational efficiency: Core strategies. 2024 [cited 2024 Oct 30]. Available from: <https://eyer.ai/blog/ai-for-operational-efficiency-core-strategies/>

30. Sphere Partners. Enhancing operational efficiency through AI integration and data modernization. 2024 [cited 2024 Oct 30]. Available from: <https://www.sphereinc.com/case-studies/enhancing-operational-efficiency-through-ai-integration-and-data-modernization/>

31. Madaoui N. The impact of artificial intelligence on legal systems: Challenges and opportunities. *Problems of Legality*. 2024;1(164):285-303. <https://doi.org/10.21564/2414-990x.164.289266>

32. Kulal A, Rahiman HU, Suvarna H, Abhishek N, Dinesh S. Enhancing public service delivery efficiency: Exploring the impact of AI. *J. Open Innov. Technol. Market and Complexity*. 2024:100329. <https://doi.org/10.1016/j.joitmc.2024.100329>

33. Vitanov P. Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters. *Eur. Parliament*. 2021 [cited 2024 Oct 30]. Available from: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

34. Hubanova T, Shchokin R, Hubanov O, Antonov V, Slobodianiuk P, Podolyaka S. Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine. *J. Inf. Technol. Manage*. 2021;13:75-90. <https://doi.org/10.22059/JITM.2021.80738>

35. Beshay. Growing public concern about the role of artificial intelligence in daily life. *Pew Res. Center*. 2024 [cited 2024 Oct 30]. Available from: <https://www.pewresearch.org>

FINANCING

None.

CONFLICT OF INTEREST

None.

AUTHORSHIP CONTRIBUTION

Conceptualization: Oleksadr Herasymenko, Volodymyr Artemov, Oleksii Kravtsev, Oleksandr Yunin, Yaroslav Fedorchuk.

Data curation: Oleksadr Herasymenko, Volodymyr Artemov, Oleksii Kravtsev, Oleksandr Yunin, Yaroslav Fedorchuk.

Research: Oleksadr Herasymenko, Volodymyr Artemov, Oleksii Kravtsev, Oleksandr Yunin, Yaroslav Fedorchuk.

Methodology: Oleksadr Herasymenko, Volodymyr Artemov, Oleksii Kravtsev, Oleksandr Yunin, Yaroslav Fedorchuk.

Project administration: Oleksadr Herasymenko, Volodymyr Artemov, Oleksii Kravtsev, Oleksandr Yunin, Yaroslav Fedorchuk.

Writing - original draft: Oleksadr Herasymenko, Volodymyr Artemov, Oleksii Kravtsev, Oleksandr Yunin, Yaroslav Fedorchuk.

Writing - revision and editing: Oleksadr Herasymenko, Volodymyr Artemov, Oleksii Kravtsev, Oleksandr Yunin, Yaroslav Fedorchuk.

APPENDIX A

QUESTIONNAIRE

SECTION 1. DEMOGRAPHIC AND PROFESSIONAL BACKGROUND

1. What is your current position? (*AI specialist, security manager, law enforcement officer, other - specify*)
2. How long have you been in this position?
 - Less than 1 year
 - 1-3 years
 - 4-6 year old
 - 7-10 years
 - More than 10 years
3. In which sector do you work? (*Energy, transport, telecommunications, water treatment, production, other - specify*)
4. In which region of Ukraine do you live?

CHAPTER 2. AI ACCEPTANCE AND IMPLEMENTATION

1. How long has AI been used in your organization's security?
 - Less than 1 year
 - 1-2 years
 - 3-5 years
 - More than 5 years
2. What AI tools are currently being used in your organization? (*Please select all that apply*)
 - Face recognition
 - Video surveillance analytics
 - Predictive control algorithms
 - Anomaly detection systems
 - Threat analysis platforms
 - Other - specify

SECTION 3. EFFECTIVENESS OF THE AI SYSTEM

1. How effective have AI tools been in reducing crime at your company?
 - Very effective
 - Effective
 - Moderately effective
 - Ineffective
 - Very ineffective
2. What specific improvements have you seen since implementing AI? (*Choose all that apply*)
 - Reduction of security breaches
 - Faster response time to incidents
 - Improved threat detection
 - Increased accuracy of identifying suspects
 - Better allocation of resources
 - Other - specify
3. Can you give an example of a successful intervention or incident that was directly impacted by AI tools? (*Open*)
4. How has AI affected the workload of security personnel?
 - Significantly reduced
 - Somewhat reduced
 - No changes
 - Somewhat increased
 - Increased significantly

SECTOR 4: CHALLENGES AND LIMITATIONS

1. What challenges did your organization face when implementing AI systems? *(Choose all that apply)*
 - High costs
 - Technical difficulties
 - Staff resistance
 - Insufficient training
 - Data privacy concerns
 - Integration with existing systems
 - Other - specify

2. How would you rate the level of support provided by AI vendors or technology partners during the implementation process?
 - Excellent
 - Good
 - Medium
 - Poor
 - Very bad

3. Have you faced any legal or regulatory issues related to the deployment of AI in your organization? *(Yes/No - if yes, please explain)*

4. What are the main limitations of AI systems currently in use? *(Open)*

SECTION 5. FURTHER PROSPECTS AND RECOMMENDATIONS

1. In what areas do you see the potential for further integration of AI in your organization? *(Please select all that apply)*
 - Cyber security
 - Physical security
 - Resource management
 - Risk assessment
 - Responding to emergency situations
 - Other - specify

2. What improvements or upgrades would you recommend for existing AI systems? *(Open)*

3. How do you see the role of AI in law enforcement and critical infrastructure protection over the next 5 years? *(Open)*

4. Would you recommend continuing or expanding the use of AI in your organization?
 - Strongly recommend
 - I recommend
 - Neutral
 - I do not recommend
 - Strongly do not recommend

SECTION 6. ETHICAL AND SOCIAL CONSIDERATIONS

1. Are there ethical issues related to the use of AI in your organization? *(Yes/No - if yes, please describe)*

2. How does your organization deal with privacy and data protection when using AI tools? *(Open)*

3. What is the general perception of AI among your colleagues?
 - Very favourable
 - Favourable
 - Neutral
 - Unfavourable
 - Very unfavourable

4. What measures are taken to ensure that AI systems are used responsibly and ethically in your organization? *(Open)*