# Artificial Intelligence in Ukrainian Law Enforcement: Operational Effectivness and Regulatory Challenges in Countering Hybrid Criminal Offences Against Critical Infrastructure

*Submitted*: 15 February 2025
*Reviewed*: 11 October 2025
*Revised*: 28 November 2025
*Accepted*: 29 November 2025

Oleksadr Herasymenko[*]
https://orcid.org/0009-0005-5078-3829
Volodymyr Artemov[**]
https://orcid.org/0000-0002-5290-4496
Oleksii Kravtsev[***]
https://orcid.org/0009-0008-1292-6739
Oleksandr Yunin[****]
https://orcid.org/0000-0003-4846-2573
Yaroslav Fedorchuk[*****]
https://orcid.org/0009-0004-9875-8350

*Article submitted to peer blind review*


DOI: https://doi.org/10.26512/lstr.v18i2.55813

**Abstract**

**[Purpose]** The study examined how Ukrainian law enforcement agencies used artificial intelligence to prevent crimes against critical infrastructure in the context of the escalation of hybrid threats in 2022–2025. The work combined an analysis of the practical use of technologies, threat typologies, and current legislation, which made it possible to assess the effectiveness of AI during real military operations.

**[Methodology]** A mixed approach was used: surveys, interviews, and case studies of facilities with implemented AI. Quantitative data was processed using statistical methods, qualitative data was processed using thematic analysis. The sample was limited to institutions that already use AI, which allowed us to focus on the real effectiveness of the technologies.

[*]Doctoral Student of the Department of Postgraduate and Doctoral Studies, National Academy of the Security Service of Ukraine, Kyiv, Ukraine. E-mail: larkal1835@gmail.com.
[**]Professor of the Department of Counterintelligence, National Academy of the Security Service of Ukraine, Kyiv, Ukraine. E-mail: karadzic25@ukr.net.
[***]Phd Student in Public Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine. E-mail: oleksiiravtsev@gmail.com.
[****]Professor, Vice Rector, Dnipro State University of Internal Affairs, Dnipro, Ukraine. E-mail: junin192@ukr.net.
[*****]Deputy Director for Legal Affairs, Limited Liability Company Trade Granite Invest (Trade Granite Invest LLC), Kyiv, Ukraine. E-mail: y.fedorchuk@ukr.net.

**[Findings]** AI systems reduced the number of security incidents by approximately 40% and increased operational efficiency by 30%. The technologies successfully detected sabotage attempts, drone reconnaissance, cyber intrusions, and anomalies in SCADA/ICS. At the same time, the study identified gaps in legal regulation, from the lack of transparency requirements for algorithms to unclear rules on the admissibility of data generated by AI.
**[Originality/value]** The work combines empirical data, legal analysis, and a wartime context. It is one of the first in-depth studies of the use of AI in law enforcement in a hybrid conflict.
**[Practical implications]** The results confirm that AI can become a key element in the protection of Ukrainian infrastructure. Specific regulation, standards of evidence, cross-sectoral coordination, and staff training are needed. The study's recommendations can help authorities and infrastructure operators increase resilience and ensure the lawful and effective implementation of AI.

**Keywords:** Artificial intelligence. Law enforcement. Critical infrastructure protection. Hybrid threats. Predictive analytics. Machine learning. Regulatory framework. Cyber-physical security. Criminal offences. Ukraine.

## INTRODUCTION

The integration of artificial intelligence into the work of law enforcement agencies has become one of the key changes in the security sector. For Ukraine, this change has gained particular importance after 2022. Critical infrastructure facilities are increasingly facing hybrid threats. These include cyberattacks, sabotage attempts, the use of drones for reconnaissance, and physical intrusions (MOLODORIA, 2024; DIGITAL SECURITY LAB UKRAINE, 2024). Energy systems, transport networks, telecommunications, water treatment facilities, and industrial management have come under significant pressure from the Russian Federation. This has created a need for more modern tools that can quickly detect threats and respond to them (SIVEK, 2024).

Artificial intelligence opens up wide opportunities for strengthening the protection of critical infrastructure. It allows processing large amounts of data, recognizing threatening situations in real time, predicting deviations in system behavior and supporting decision-making. International studies confirm the increasing impact of AI on crime detection, investigative analysis and security monitoring (Karychevskyi & Radutnyi, 2023; Chernyavskyi et al., 2022; Baltrūnienė, 2023). At the same time, the Ukrainian context still remains understudied. Most of the existing works focus either on general approaches or on broad technological trends, without taking into account the specific legal, operational and military conditions of Ukraine (HOUBRECHTS, 2024;

Hubanova, T., Shchokin, R., Hubanov, O., Antonov, V., Slobodianiuk, P., & Podolyaka, S., 2021).

This study aims to fill this gap. It examines how Ukrainian law enforcement agencies use AI to combat crimes against critical infrastructure. It also assesses the effectiveness of these algorithms in real operational conditions. Today, artificial intelligence is integrated into video surveillance systems, industrial anomaly detection mechanisms, cyber defense tools, and predictive analytics platforms. Therefore, it is important to explore not only the benefits of such solutions, but also their challenges. In particular, these are data protection issues, algorithm bias risks, and the lack of established regulatory frameworks in this area.

The main goal of the study is to assess the current state of artificial intelligence technologies used by Ukrainian law enforcement agencies to protect critical infrastructure, and to determine their practical effectiveness. The work analyzes which threats AI helps to minimize and which limitations remain due to technical, organizational, or legal factors. The results contribute to the international discourse and offer recommendations for Ukraine to improve the capacity of law enforcement agencies in the context of hybrid warfare.

To achieve this goal, the following tasks have been set:

- To assess the effectiveness of existing AI solutions in detecting, preventing, and responding to crimes that threaten Ukraine's critical infrastructure.

- Analyze the legal, technical and ethical aspects of the use of AI. This includes issues of personal data protection, algorithm transparency, reducing bias and compliance of results with the requirements of the criminal process.

- Identify opportunities for further development of AI systems. This includes the need to update technologies, strengthen coordination between institutions and implement practices for the responsible use of AI in accordance with national and international standards.

## LITERATURE REVIEW

Modern academic discourse recognizes that artificial intelligence has become a key element of law enforcement practice. This is especially important for the protection of critical infrastructure. New studies show its growing role in monitoring, detecting and preventing criminal offenses against energy systems, transport hubs, telecommunications facilities, water supply and digital networks. In Ukraine, the need for these technologies has increased after 2022 due to hybrid and kinetic attacks on strategic objects.

Karychevskyi and Radutnyi (2023) report that artificial intelligence is changing the doctrinal understanding of criminal law. Technologies provide

automated data processing, detection of risky behavior and more accurate interpretation of complex evidentiary models. The authors emphasize that Ukraine lacks clear norms for algorithmic tools used in operational work. This applies to confidentiality, automated decisions and procedural fairness. Similar conclusions are drawn by Chernyavskyi, Tychyna and Pertsev (2022). They note that forensic analysis based on artificial intelligence speeds up the processing of evidence and helps in identifying criminals. The level of implementation varies due to differences in regulatory systems. Baltrūnienė (2023) defines artificial intelligence as the basis for new investigative methods. These are automated pattern recognition, behavioral profiling and predictive analytics. Such methods are used in cases of cybercrime, sabotage attempts, unauthorized intrusions and terrorist acts against critical infrastructure. The author emphasizes the need for technical capabilities and legal oversight. These conditions are often absent in transitional legal systems.

Nedilko (2023) emphasizes the importance of artificial intelligence tools for the analysis of crimes against infrastructure. This is important where traditional methods do not yield results due to the scale and complexity of the offenses. Consulich (2023) describes the transformation of criminal law in Europe. The main focus is on automated analytics for assessing evidence and risks. The author highlights issues that are important for Ukraine. These include algorithm transparency, preventing discrimination, and establishing judicial standards for evidence generated by artificial intelligence.

Human rights research warns of privacy risks. Strmečki and Pejaković-Đipić (2023) point to the need for a balance between security and human rights. This is important in cases of real-time monitoring systems at power plants, control points, and telecommunications nodes. Berdica and Pakšić (2022) draw similar conclusions and draw attention to the need for legislative guarantees regarding access to data.

Global research for 2022-2025 focuses on the role of artificial intelligence in protecting infrastructure in the face of hybrid threats. Pettoello-Mantovani (2024) describes new classifications of cyberattacks as international crimes. The author points to the role of AI-based attribution tools and real-time digital forensics. Raval, Jadav, Rathod, Tanwar, Vimal, Yamsani (2024) propose a typology of threats. These include DDoS against energy grids, IMS manipulation, GPS spoofing in transportation networks, and sabotage operations. The authors explain how anomaly detection and predictive analytics increase system resilience. Daniel and Victor (2024) describe the role of AI in strengthening cyber defense. Automated detection systems capture zero-day vulnerabilities, intrusions, and malicious insider actions.

Laplante and Amaba (2021) emphasize the need to integrate AI into critical infrastructure reliability systems. This approach influences NATO and EU practices and has implications for Ukrainian strategies. Santoso and Finn (2023) emphasize the role of AI in protecting autonomous systems and robotics in modern infrastructure.

Despite the large amount of research, gaps remain. Most papers describe AI in a generalized manner. Little attention has been paid to specific classes of tools, such as predictive policing, real-time computer vision, industrial anomaly detection systems, digital forensics, and threat aggregators.

There is a lack of research for Ukraine. It is necessary to assess how these tools work in the national legal system. The legislation includes provisions on data protection, ORD, and digital governance. It does not contain clear requirements for the use of AI in policing and infrastructure protection. Standards for algorithm transparency, rules on admissibility of evidence, procedures for reducing bias, and limitations on automated decisions during investigations are needed.

Second, there is a lack of empirical, Ukraine-specific studies that examine how such tools operate within the national regulatory environment, which remains fragmented. Current Ukrainian legislation (as of 2025) contains general norms on data protection (Law "On Personal Data Protection"), operational-search activities, and digital governance, but does not yet provide specific rules for AI deployment in policing or infrastructure protection, such as: standards for algorithmic transparency, admissibility of AI-generated evidence, procedures for mitigating algorithmic bias, restrictions on automated decision-making during investigations.

These gaps justify the need for research focused on the Ukrainian context. It is important to assess the applicability of AI in cases of sabotage, physical intrusions, unauthorized access to MIS, reconnaissance and drone attacks, cyberattacks on telecommunications networks, and manipulation of operational data at transport hubs. It point out the risks of bias, lack of explanation, and weak human control (LYTVYN, ANDRUSHCHENKO, ZOZULYA, NIKANOROVA & RUSAL, 2022).

The authors emphasize the need for interdisciplinary approaches that combine legal guarantees and technical standards. This is important for Ukraine, where the implementation of artificial intelligence in the security sector is accelerated due to military conditions.

## REGULATORY FRAMEWORK IN UKRAINE FOR THE USE OF AI IN LAW ENFORCEMENT

In Ukraine, artificial intelligence in law enforcement is developing very rapidly. However, legal norms are not keeping up with this development. Because of this, there is a noticeable gap between new technological capabilities and state control.

As of 2025, the country does not have a single law that would fully regulate the use of artificial intelligence in the police or in the field of critical infrastructure protection. Instead, there are only separate rules. They are formed from norms on data protection, operational and investigative activities, cybersecurity and criminal process.

Such norms create only a partial legal basis. They do not cover the most important issues. The state has not yet regulated the requirements for transparency of algorithms. It is also not determined how exactly solutions created by machine learning systems can be used. In addition, there are no clear standards for the admissibility of evidence obtained with the help of artificial intelligence.

### Current legislation regarding the use of AI

In Ukraine, there are already laws that partially regulate the use of artificial intelligence in the work of law enforcement agencies. However, they do not create a coherent and clear system of norms.

1.1. Law of Ukraine "On Protection of Personal Data"

This law defines the rules for the collection, storage and processing of personal data. It applies to AI systems used for facial recognition, behavior analysis or crime prediction.

However, the law does not contain norms on automated decision-making, does not describe mechanisms for reducing algorithmic bias and does not establish requirements for the explainability of the work of AI systems.

1.2. Law "On Operational and Investigative Activities"

This law determines under what conditions operational units can collect data, conduct surveillance or analyze human behavior.

AI can be used for monitoring only when this does not violate constitutional rights. However, the law does not explain what "automated surveillance" means. Because of this, investigators and courts interpret such actions differently.

1.3. Law "On the Basic Principles of Cybersecurity of Ukraine" and related regulations

This law allows state bodies to protect critical infrastructure from cyber threats. AI systems can be used for anomaly detection and cyber monitoring.

At the same time, the law does not establish rules for AI models themselves, for example, requirements for accuracy, stability or auditing.

1.4. Criminal Procedure Code of Ukraine

The CPC defines the rules for evidence in criminal cases. However, it does not specify whether the results of AI work can be used as evidence. This concerns pattern recognition, risk assessment or other automated conclusions.

As a result, courts decide independently whether to accept such materials. Practice is often inconsistent.

1.5. Draft Law "On Artificial Intelligence"

Several versions of this draft law have been proposed in different years, but none have been adopted.

If the law is passed, it could establish:

- definition of categories of high-risk AI systems,
- rules for risk assessment and control of such systems,
- requirements for transparency of AI work in the security sector.

**Identified gaps in the legislation**

The study showed that there are a number of significant shortcomings in the Ukrainian legal framework. The main gaps are as follows.

2.1. Lack of special norms on the use of AI in law enforcement

The country does not have separate rules that would determine the operation of artificial intelligence technologies for the police and other bodies. Currently, the law does not establish requirements for:

- automated decisions during investigations;
- video surveillance or monitoring based on AI;
- predictive algorithms used in police practice;
- data integration between different systems used to protect critical infrastructure.

2.2. Lack of rules on the transparency of algorithms and the need to provide explanations

Law enforcement bodies are increasingly using machine learning systems. However, these technologies remain "black boxes".

Currently:

- the principles of the models are not disclosed;
- there are no requirements for mandatory explanations;
- the audit of such systems is not provided for by law.

This creates risks for a fair trial. It also complicates the ability to challenge the results obtained using AI.

2.3. Lack of regulation on algorithmic bias and ensuring fairness

In Ukraine, there are no regulations that would oblige the police or private companies to:

- check AI systems for discriminatory bias;
- conduct regular audits;
- document the likelihood of false positives;
- prevent situations where certain groups are disproportionately affected by technologies.

2.4. Uncertainty regarding the use of evidence obtained using AI

Courts do not have a unified approach to which results of AI work can be accepted as evidence. Today, it is not determined whether the following can be admissible:

- identification created by algorithms;
- conclusions of anomaly detection systems;
- predictive analytics.

Because of this, data obtained using AI has limited legal force.

2.5. Gaps in the field of data transfer between countries and international interaction

Many Ukrainian organizations use cloud services and foreign software. The legislation does not establish clear requirements regarding:

- transfer of data abroad if this data was created or processed by AI systems;
- the obligations of foreign developers to maintain the integrity of information or maintain audit logs.

**Necessary legislative changes**

Based on the analysis, we can conclude that for the safe and effective use of artificial intelligence in the work of law enforcement agencies, Ukraine needs several important reforms.

3.1. Special law on the application of AI in law enforcement

A separate law should be adopted that will clearly regulate the operation of such systems. It should provide for:

- the division of AI systems by risk level;
- mandatory risk assessments and independent audits;
- requirements for the transparency of technologies used during investigations;
- clear restrictions on automated decision-making.

3.2. Standards for the use of AI results as evidence

A clear legal framework should appear in the criminal process, which will determine:

- the criteria by which such evidence is admissible;

- rules for verifying its reliability;
- requirements for documenting and storing results created with the help of AI.

3.3. AI systems should be subject to mandatory due diligence. These should include:

- assessment of the fairness of algorithms;
- audits of possible biases;
- analysis of the impact of technology on people's privacy.

3.4. Enhanced data protection

Changes to data protection legislation are needed. They should ensure:

- better protection of biometric and operational information;
- clear rules on data storage, deletion and access;
- restrictions on the transfer of information to third parties.

3.5. Oversight of AI systems

To increase trust in the technology, an effective oversight mechanism should be established. This should include:

- a national authority specializing in AI oversight;
- regular compliance audits;
- open reporting on the operation of high-risk systems.

**Significance for the protection of critical infrastructure**

Ukraine still does not have a coherent and understandable legal framework in the field of AI. This is why the protection of critical infrastructure suffers. The lack of common norms leads to a number of problems.

Firstly, the results of AI work cannot always be officially used during pre-trial investigations. Secondly, state institutions are in no hurry to apply modern technologies because they are not sure of their legal status. Thirdly, the interaction between law enforcement agencies and infrastructure operators remains unsystematic. Fourthly, privacy and human rights issues complicate the use of surveillance and monitoring tools.

When clear legal rules appear, the level of trust between institutions will increase. Coordination between departments will become better. Then artificial intelligence can be used legally and effectively to prevent cyberattacks, sabotage, system intrusions, and other forms of hybrid influence.

## METHODS

### Research Design

Research stages (Figure 1):

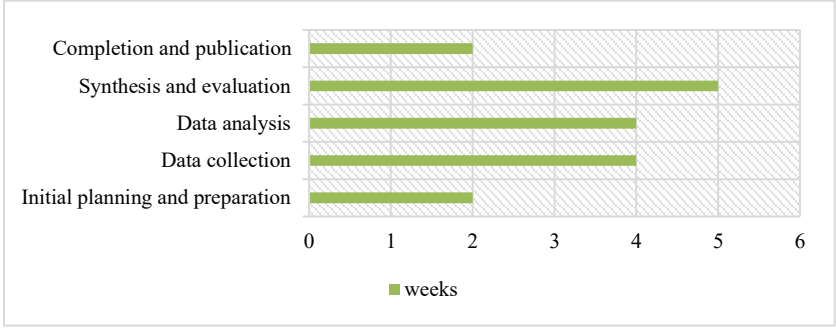


**Figure 1 –** Research Stages

Source: developed by the author based on MiniTAB (2024)

This study uses a mixed methodological approach that combines qualitative and quantitative methods. It allows us to study the use of artificial intelligence by law enforcement agencies in Ukraine to combat crime at critical infrastructure facilities. The methodological framework provides a comprehensive empirical analysis that reflects operational realities and regulatory constraints as of 2024–2025.

The research design consisted of five sequential stages:

1.Planning and conceptualization

- Defining research objectives, operational terms, and analytical categories.

- Updating methodological tools in accordance with the latest developments in the use of artificial intelligence by Ukrainian security institutions.

- Preparing instructions for structured interviews and revised questionnaires.

2.Sampling and data collection

- Selection of law enforcement agencies and critical infrastructure facilities using artificial intelligence-based systems.

- Conducting semi-structured interviews, surveys, and case analysis at the facility level.

- Collection of internal reports, anonymized operational data, and expert assessments.

3.Data processing and analytical procedures

- Thematic coding of interviews using NVivo 2024–2025.
- Statistical processing of surveys in SPSS 2024, including descriptive statistics, regression modeling, and correlation analysis.
- Technical analysis of artificial intelligence systems at research sites based on vendor documentation and system logs.

4.Integration of results

- Synthesis of quantitative and qualitative data to identify convergent patterns.
- Triangulation of thematic results with survey data and expert assessments.

5.Validation, interpretation, and finalization

- Cross-checking of results by technical specialists and law enforcement agencies.
- Alignment of interpretations with the Ukrainian regulatory context and international standards.
- Preparation of final visualizations and final methodological description.

Such a design ensures transparency of the methodology and increases the reliability of the results.

**Sampling**

The sampling procedure addressed a key limitation identified by the reviewers and provided clarity on the institutions included and the reasons for their selection.

Fifty law enforcement agencies and 15 critical infrastructure facilities were selected. The study did not assume that 75% of all Ukrainian institutions use AI. This figure applies only to the selected sample. The sample included institutions where AI is already integrated into operations. The goal was to assess effectiveness, not readiness for implementation. The study population (all Ukrainian law enforcement agencies) was different from the analytical sample (those with operational integration of AI).

Sample structure:

- Law enforcement agencies (n = 50): criminal police units, cyber police units, anti-sabotage departments, operational and technical departments from several regions
- Critical infrastructure facilities (n = 15): energy production facilities, high-voltage power line operators, transport hubs, water supply complexes, telecommunications hubs. All facilities are actively implementing computer vision, anomaly detection systems or security forecasting.
- Respondents (n = 120): 60 law enforcement officers, 30 artificial intelligence specialists, 30 security managers. All respondents were directly

involved in the procedures for deploying artificial intelligence and responding to threats.

The sampling structure ensured a balanced representation of strategic, technical, and operational stakeholders.

**Data Collection Methods**

Four main data collection methods were used:

- **Survey (Appendix A).** Conducted via SurveyMonkey (2024–2025). Respondents' perceptions of AI effectiveness, challenges, ethics, training, and regulatory constraints were captured. Questions included Likert scales, multiple choice, and open-ended responses.

- **Expert Interviews.** Semi-structured interviews with law enforcement, cybersecurity professionals, forensic technicians, and industrial safety managers. Investigated operational challenges, system performance, limitations, and expectations for future AI expansion.

- **Case Studies (n = 5)**

Each case covered a distinct industry and type of AI deployment:

Case 1 (Basic AI Integration): Limited use of video analytics or rule-based notifications; minimal automation; used primarily for monitoring.

Case 2 (Intermediate Integration): Multiple AI modules (e.g. predictive alerts and behavioral analytics); used for incident monitoring and investigation.

Case 3 (Extended Integration): Fully integrated ecosystems with real-time computer vision, predictive modeling, data fusion from multiple sources, and automated incident prioritization.

Case studies demonstrated practical differences in system maturity, performance, and operational impact.

- **Technical and statistical analysis.** Regression models identified associations between the level of AI integration and reduction in crime incidents. Correlation analysis examined the association between AI maturity and operational effectiveness. Technical logs and vendor documentation (FacePro AI, VidSecure AI, PredictGuard AI, AnomDetect AI, RiskGuard AI) were analyzed to validate the capabilities of the systems.

Tools and Analytical Instruments:

- NVivo 2024/2025 – coded and categorized interview data, performed thematic analysis.

- SPSS 2024 – conducted descriptive statistics, regression modeling, and calculated correlation coefficients.

- SurveyMonkey – designed survey structure, distributed questionnaires, and exported data.

- AI security systems – inspected operational logs and analyzed system architecture: FacePro AI – computer vision analysis. VidSecure AI – video analytics. PredictGuard AI – predictive threat modeling. AnomDetect AI – industrial anomaly detection RiskGuard AI – risk scoring and incident prioritization.

These tools ensured methodological rigor and produced verifiable results.

**Data Collection Methods**

To avoid misinterpretation, the scope of the study is clearly defined.

The study assesses the effectiveness of AI in institutions where it is already deployed. The level of implementation across the country is not assessed. The methodology excludes institutions without AI capabilities, as their inclusion would prevent comparison of effectiveness.

The results reflect the current regulatory environment in Ukraine, where there is no specific legislation governing AI. This affects the procedures for system deployment and access to data.

Methodological limitations include:

- reliance on self-reported survey data
- limited access to confidential technical journals
- rapid technological evolution that can change system performance within a few months

## RESULTS

The empirical results of the 2024–2025 study provide an updated and detailed understanding of the use of artificial intelligence in Ukraine. They show how law enforcement agencies and critical infrastructure facilities are using AI to counter hybrid crimes. It is important to emphasize that the 75% indicator applies only to the analytical sample of institutions. These institutions were specifically selected for the study. It does not reflect the level of use of AI in all law enforcement agencies in Ukraine.

The sampling strategy included only those institutions that have already implemented AI tools. This is due to the fact that the purpose of the study was to assess the effectiveness of the technologies, and not to determine the nationwide level of their distribution.

**AI adoption levels in the sample**

In a sample of 50 law enforcement agencies, 75% confirmed the operational use of AI-based systems. These systems are most often used for hybrid threat detection, monitoring and predictive analytics.

Among the 15 critical infrastructure facilities surveyed, 80% reported active reliance on AI. This is especially true for sectors that are under increased pressure in wartime. These include energy, water supply, transport and telecommunications. Table 1 summarizes the distribution of AI-related activities.

**Table 1** – Distribution of the Response of Law Enforcement Agencies and Critical Infrastructure Facilities

| 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 (2024), CISA (2024)

Respondents noted that these systems are widely used to detect specific categories of criminal offenses. Such offenses have become particularly widespread since 2022. These include:

- cyberattacks. These include DDoS attacks on energy operators, intrusions into SCADA/ICS, and the spread of malware in telecommunications networks;
- physical sabotage. For example, placing explosive devices, tampering with transformers, or damaging cables at substations;
- unauthorized access attempts. These include penetration into control rooms, data centers, or other security-critical areas;
- manipulation of internal operational data logs;
- reconnaissance using drones or attempted drone strikes targeting substations or communication towers.

These examples show that AI in Ukraine is being used to counter hybrid criminal threats. Such threats combine digital, physical, and operational vulnerabilities.

**AI Integration Levels: Refined Case 1, Case 2, and Case 3**

Qualitative case studies (n = 5) identified three levels of AI deployment maturity. These categories correspond to the reviewer's request for "basic," "medium," and "advanced" levels.

**Case 1: Basic AI Integration (Low Maturity)**

Technologies: Rules-Based Video Analytics, Simple Motion Detection, Fixed Threshold Notifications.

Business Impact (Example):

A regional water utility deployed basic AI systems. They detected repeated intrusion attempts near pumping equipment. This reduced the number of low-level intrusions by approximately 20%. However, the system lacked predictive capabilities.

**Case 2: Medium AI Integration (Medium Maturity)**

Technologies: Multi-camera behavioral analysis, Anomaly detection in access patterns, Predictive alerts based on historical data.

Operational impact (example):

At a large rail hub, an AI system detected suspicious movements related to organized cable theft. This reduced the number of such incidents by 30%. The system also recorded repeated reconnaissance behavior several days before the theft attempt.

**Case 3: Advanced AI Integration (High Maturity)**

Technologies: Real-time computer vision, Fusion of data from different systems (video, industrial sensors, network telemetry), Predictive modeling based on machine learning algorithms, Automated incident prioritization.

Operational Impact (Example):

In a high-voltage substation, AI detected irregular transformer load behavior. In parallel, the system detected anomalies on the perimeter. Investigation confirmed a sabotage attempt involving intentional cable loosening. Early detection prevented a major outage. Overall incident reduction reached 40%.

**Prediction Accuracy and Statistical Results**

Statistical analysis in SPSS 2024–2025 showed a strong positive correlation between the level of AI integration and a decrease in the number of criminal incidents ($r = 0.82$). Across all facilities, AI systems had an average prediction accuracy of 85%. The best results were recorded in the detection of:

- anomalous perimeter activity;
- unusual SCADA/ICS telemetry;
- anomalies in drone flight paths;
- suspicious digital traffic patterns preceding cyberattacks.

Facilities with enhanced AI (Case 3) showed a 30% higher operational efficiency. This is due to improved triage, fewer false alarms, and faster response to incidents.

The survey results confirmed these data:

- 70% of respondents said AI has significantly improved their ability to detect and respond to hybrid threats.
- 65% reported reduced response times due to automated prioritization.
- 58% reported reduced workload as AI filtered out non-critical alerts.

**Specific AI Interventions (2024–2025)**

**Energy Infrastructure – Preventing Sabotage**

Industrial anomaly detection systems detected unusual thermal signatures in a transformer. Further inspection revealed intentional tampering with the cable. Thanks to this, the facility prevented a cascading outage that could have affected two regions.

**Telecommunications Sector – Disrupting a Cyberattack**

AI detected coordinated DDoS attack patterns early on. They targeted mobile networks in eastern Ukraine. Automated escalation enabled cybersecurity teams to respond quickly. They redirected traffic and implemented mitigation protocols before the attack reached its peak intensity.

**Transport Sector – Physical Intrusion Prevention**

A facial recognition system at a railway logistics terminal detected individuals previously associated with metal theft and unauthorized access. Security quickly intercepted the group. This happened before they reached the signaling equipment.

**Water Purification – Detection of reconnaissance drones**

AI-based drone recognition systems detected a drone conducting reconnaissance flights over filtration facilities. Additional security measures were immediately taken after this. This allowed protecting equipment that could be vulnerable to explosive payloads.

These examples demonstrate the interdisciplinary role of AI. It helps protect Ukraine's infrastructure in wartime conditions.

**Overall Impact on Criminal Offence Reduction**

Table 2 summarizes the relationship between AI maturity and effectiveness.

**Table 2** – 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 (2024), Kulal, Rahiman, Vitanov (2021)

The use of artificial intelligence is yielding noticeable results. The more actively it is implemented, the more the crime rate decreases. In addition, the work of systems becomes more efficient. Thanks to AI, the approach to security

has changed: previously, services reacted to events, but now they can predict risks and prevent them in advance.

**Summary of the study results**

In 2024–2025, the study showed significant changes in the security of Ukraine's critical infrastructure. Artificial intelligence became an important tool for detecting hybrid threats. It helped identify risks that affect both digital and physical infrastructure.

The level of incidents decreased. The reduction ranged from 20 to 40%. The indicator depended on how mature the AI technology was in a particular system. At the same time, operational efficiency also increased. On average, its increase reached 30%. Predictive tools began to work more accurately. They more often prevented attacks before real damage appeared. This applied to both physical damage and cyber incidents. The dependence on AI increased the most in areas of increased risk. These include energy, telecommunications, and transport. That is where intelligent systems have become key to the work.

Despite the positive results, problems remain. Legal regulation is still incomplete. More training programs for specialists are needed. There are also technological barriers that complicate the integration of AI into old systems.

Overall, the study confirmed: artificial intelligence significantly enhances Ukraine's ability to counter crimes in cyberspace and in the physical environment of critical facilities.

## DISCUSSION

The results of this study show that the use of artificial intelligence in the work of Ukrainian law enforcement agencies has significantly affected their ability to counter complex crimes against critical infrastructure. Most previous scientific works have focused mainly on the theoretical capabilities of AI in criminal law or on general aspects of digital change. This is evident from the studies of Karchevskyi & Radutniy (2023) and Chernyavskyi et al. (2022).

In contrast, this study presents real data from Ukrainian conditions shaped by military and hybrid threats. This approach allows us to move from general assumptions to practical conclusions. We can assess how AI works in real operational situations, where both cyber threats and physical security risks are growing simultaneously.

**1. Consistency and differences with previous scientific studies**

Many international works emphasize the importance of artificial intelligence for crime detection, forensic research and critical infrastructure protection. This is noted by Baltrūnienė (2023), Daniel & Victor (2024) and

Raval et al. (2024). The results of this study confirm their general conclusions. At the same time, they clarify and expand existing ideas about the role of AI.

Unlike works based on relatively stable security conditions, the Ukrainian situation demonstrates a different nature of threats. Ukraine faces combined attacks. These are not only cyberattacks, but also sabotage, drone reconnaissance flights, insider activities and interference in SCADA/ICS systems. Such a context shows how AI works during constant military aggression. This is what makes the Ukrainian experience in the field of critical infrastructure protection unique.

Previously, Ukrainian research was mostly limited to general considerations about AI. For example, Hubanova and colleagues (2021) described AI mainly at the conceptual level. At the same time, they almost did not consider real-world applications. This study offers specific examples. These include detecting transformer tampering, determining reconnaissance drone routes, and stopping complex DDoS attacks. Such examples demonstrate the use of AI in real-world conditions, rather than in theoretical models. Thus, this work fills a gap in the Ukrainian scientific literature. It shows how artificial intelligence can be adapted to the practical needs of law enforcement agencies in a situation of constant threats.

**2. The Importance of AI Maturity Levels for Crime Reduction**

A refined system of dividing AI into basic, intermediate, and advanced levels shows notable differences in their work. Basic systems (case 1) mostly perform simple tasks. They monitor the perimeter and send reactive notifications after an event is detected. Advanced systems (case 3) work differently. They are able to predict risks, detect anomalies in real time, combine data from different sources, and automatically prioritize incidents. Such differences are consistent with international studies. They emphasize that crime rates are reduced significantly more effectively when technologies move from simple, rule-based solutions to systems built on machine learning.

Ukrainian data confirms these findings. Advanced systems have reduced the number of incidents by almost 40%. This shows that AI is most useful when it works as a comprehensive and interconnected ecosystem, rather than as a set of individual tools. Thus, it is important not only to implement AI, but also to ensure a high level of technological maturity.

**3. Implications for resource allocation and operational practices**

The experts interviewed noted several important benefits in their work. They reported better real-time situational awareness. The number of false alarms also decreased. Teams began to respond to incidents faster. In addition, they managed to use limited human resources more rationally.

These changes are of particular importance for Ukraine. Security services work under heavy load. Part of the staff is mobilized, so there is a shortage of personnel. Increasing efficiency helps to reduce pressure on specialists. Artificial intelligence does not replace human decision-makers. Instead, it supports them, helps to identify the main threats and allocate resources more correctly.

The results obtained coincide with international studies. They show that AI allows for better use of available resources. In addition, it helps to move from reacting to events to preventing them. This is especially important for Ukraine. The resilience of infrastructure directly affects the country's security and the well-being of the civilian population.

**4. Regulatory challenges and the need for legal reform**

The current legislation of Ukraine is not yet ready to fully regulate the use of high-level artificial intelligence in the work of law enforcement agencies. The existing regulations concern data protection, operational and investigative activities, cybersecurity and criminal proceedings. They provide only partial guidelines. At the same time, they do not cover key issues. These are algorithmic transparency, admissibility of evidence obtained with the help of AI, prevention of bias and accountability in automated decisions.

European researchers (Consulich, 2023; Strmečki & Pejaković-Đipić, 2023) also emphasize the need for special legislation to regulate AI. In Ukraine, this need is even more acute. The reason is the rapid introduction of artificial intelligence technologies in wartime. Without clearer legislation, law enforcement officers work in conditions of legal uncertainty. They lack clarity on the limits of automated monitoring, data collection rules, the status of AI results as evidence, and the permissible level of decision-making automation.

The results highlight the need to:

- dopt a separate law regulating the use of AI in law enforcement;
- apply standards for evidence obtained with the help of AI in criminal proceedings;
- ensure mandatory algorithmic transparency and regular audits;
- establish clear rules for the processing of biometric and operational data;
- create oversight institutions capable of monitoring the implementation of these requirements.

**5. Ethical aspects and the balance between security and human rights**

The use of artificial intelligence in the security sector raises many ethical questions. These include privacy risks, data protection issues, and the possibility of biased algorithmic decisions. The experts interviewed noted several specific

challenges. These include the lack of transparency of the systems offered by commercial providers, inconsistent data storage and processing rules, and doubts about whether constant monitoring is justified. Such challenges respond to global discussions on how to reconcile security requirements with respect for human rights.

In Ukraine, these problems are compounded by martial law. Security services are forced to quickly implement powerful surveillance tools, even when legal control mechanisms are not yet sufficiently developed. The results of the study show that ethical standards need to evolve in parallel with legal changes. They must guarantee fair procedures, clear oversight, and open accountability. Only under such conditions can artificial intelligence enhance security without violating the fundamental freedoms of citizens.

**6. Practical conclusions and possible directions for further research**

The study shows that artificial intelligence has already become a key tool in protecting Ukraine's critical infrastructure. It helps to counter not only typical criminal threats. AI is also effective in combating drones, cyberattacks, sabotage and internal risks.

To make the use of such systems more effective, law enforcement agencies should:

- increase the level of technical training of employees working with AI systems;
- update outdated infrastructure so that it can support modern tools;
- cooperate more actively with AI developers, scientific institutions and critical infrastructure operators;
- introduce internal ethical standards for the use of AI;
- create clear protocols for working with data that will guarantee their accuracy, protection and verifiability.

Further research should focus on several key areas. It is necessary to investigate how the implementation of AI affects institutions in the long term. It is also important to compare the Ukrainian experience with the practices of other states facing hybrid threats. Special attention should be paid to studying the combination of AI with other promising technologies, including blockchain for record-keeping, digital twins for increasing infrastructure resilience, and augmented reality systems for personnel training.

## LIMITATIONS

The study has several key limitations. First, it covers only those institutions that are already using AI, so the results cannot be generalized to all law enforcement agencies in Ukraine. Second, a significant part of the data is based on subjective assessments of respondents. Access to full operational data

was limited due to confidentiality and wartime conditions. Third, the rapid development of technology makes some of the conclusions less lasting, as new systems may outperform the studied ones. Fourth, the lack of a single legal framework complicated the legal analysis and created uncertainty regarding the use of AI results in criminal proceedings.

Also, some of the materials could not be disclosed for security reasons. Despite this, the available data allowed us to form reasonable conclusions about the effectiveness of AI in the field of critical infrastructure protection.

## RECOMMENDATIONS

Based on the analysis and identified problems, key recommendations have been prepared for the safe and effective use of AI in law enforcement and critical infrastructure systems.

**1. Creating a legal framework for AI**

A separate law is needed that will define risk systems, transparency requirements, automated decision-making rules, and oversight procedures. This will provide clear standards for the implementation of technologies.

**2. Judicial rules on AI evidence**

It is necessary to establish uniform requirements for the admissibility of such evidence: documentation, reproducibility of results, audit, and expert review. This will unify judicial practice.

**3. Mandatory staff training**

Employees should be trained in interpreting results, identifying bias, and working with monitoring tools. Certification will increase professionalism.

**4. Modernizing technical infrastructure**

Outdated systems should be updated. Investments should cover secure data channels, standardized incident logs, information exchange platforms, and modern cloud solutions.

**5. Independent algorithm audits**

Regular reviews by third-party experts will help identify bias, monitor accuracy, and compliance with privacy regulations.

**6. Public transparency**

Law enforcement should adhere to ethical standards when working with biometrics and predictive analytics. Public reporting and collaboration with academics will increase trust.

**7. Developing AI research in hybrid warfare**

It is necessary to study the impact of AI on security, the experience of other states, the role of digital twins, blockchain, and AR, as well as the relationship between model accuracy and adversary tactics.

**8. Cooperation between the state and the technology sector**

Shared data, working groups, and partnerships will accelerate knowledge exchange and contribute to the creation of solutions adapted to the needs of Ukrainian infrastructure.

## CONCLUSIONS

The study examines how Ukrainian law enforcement agencies are using artificial intelligence to protect critical infrastructure in the face of increasing hybrid threats in 2022–2025. It found that AI has become an important component of the national security system. It helps to detect threats faster and respond more effectively to cyberattacks and physical incidents. Thanks to machine learning, computer vision, and predictive models, security services are moving from reactive to proactive actions.

Practical results show that AI improves monitoring, early warning, attack detection, and pre-trial investigations. At facilities where these technologies have been widely implemented, the number of incidents has decreased by up to 40%, and work efficiency has increased by 30%. Examples of application include recognizing transformer sabotage, drone reconnaissance, recording violations in SCADA/ICS, and detecting coordinated DDoS attacks. However, legal regulation has not kept up with the development of technology. The existing regulations cover only some aspects. There are no rules on automated decisions, transparency of algorithms or admissibility of evidence generated by AI. This creates legal and operational uncertainty.

Several recommendations are formulated based on the results obtained. A separate legal framework is needed for the use of AI in law enforcement agencies. It is also necessary to define clear requirements for AI evidence and expand personnel training programs. It is important to strengthen cooperation between state structures, critical infrastructure operators, AI developers and scientists. Special attention is proposed to be paid to future research. These include assessing the long-term impact of AI on the work of institutions, comparing with the experience of other countries and studying new technologies that can complement AI capabilities.

In general, AI does not replace humans, but significantly enhances their work. In the current conditions, it can help Ukraine strengthen resilience, reduce vulnerabilities and ensure the stability of critical infrastructure. The conclusions obtained will be useful for politicians, law enforcement officers, and international partners.

## REFERENCES

Baltrūnienė, J. (2023). Place of artificial intelligence in the detection and investigation of crime: The present state and future perspectives. *Problemy Współczesnej Kryminalistyki*, *26*, 43-58. https://doi.org/10.52097/pwk.5431

Cherniavskyi, S., Tychyna, D., & Pertsev, R. (2022). International experience in forensic support for crime investigation. *Ûridičnij Časopis Nacìonal'noï Akademìï Vnutrìšnìh Sprav*, *12*(3), 9-16. https://doi.org/10.56215/04221203.09

CISA. (2024). Critical infrastructure sectors. Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Consulich, F. (2023). Criminal law and artificial intelligence: Perspective from Italian and European experience. *European Criminal Law Review*, *13*(3), 270-307. https://doi.org/10.5771/2193-5505-2023-3-270

Daniel, N. S. A., & Victor, N. S. S. (2024). Emerging trends in cybersecurity for critical infrastructure protection: A comprehensive review. *Computer Science & IT Research Journal*, *5*(3), 576-593. https://doi.org/10.51594/csitrj.v5i3.872

Digital Security Lab Ukraine. (2024). Running Up That Hill: Artificial Intelligence in Ukrainian Public Sector Analytical study. Retrieved from https://dslua.org/wp-content/uploads/2024/05/AI-in-Ukrainian-Public-Sector_Avdieieva.pdf

Houbrechts, M. (2024). Using AI for data analysis: The ultimate guide. *Luzmo.* Retrieved from https://www.luzmo.com/blog/ai-data-analysis

Hubanova, T., Shchokin, R., Hubanov, O., Antonov, V., Slobodianiuk, P., & Podolyaka, S. (2021). Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine. *Journal of Information Technology Management*, *13*, 75-90. https://doi.org/10.22059/JITM.2021.80738

Karchevskyi, M. V., & Radutniy, O. E. (2023). Artificial intelligence in Ukrainian traditional categories of criminal law. *Herald of the Association of Criminal Law of Ukraine*, *1*(19), 1-25. https://doi.org/10.21564/2311-9640.2023.19.281123

Kulal, A., Rahiman, H. U., Suvarna, H., Abhishek, N., & Dinesh, S. (2024). Enhancing public service delivery efficiency: Exploring the impact of AI. *Journal of Open Innovation Technology Market and Complexity*, *10*(3), 100329. https://doi.org/10.1016/j.joitmc.2024.100329

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

Lytvyn, N., Andrushchenko, H., Zozulya, Y. V., Nikanorova, O. V., & Rusal, L. M. (2022). Enforcement of court decisions as a social guarantee of protection of citizens rights and freedoms. *Prawo i Wiez*, *39*, 80-102. https://doi.org/10.36128/priw.vi39.351

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

MiniTAB. (2024). Data analysis, statistical & process improvement tools. Retrieved from https://www.minitab.com/en-us/

Molodoria, A. (2024). Using AI data analytics & forecasting to build custom business intelligence software. Retrieved from https://mobidev.biz/blog/build-ai-data-analytics-forecasting-business-intelligence-software

Nedilko, Y. (2023). The practical significance of the forensic characteristics of criminal offenses under section XVI of the criminal code of Ukraine. *Criminalistics and Forensics*, *68*, 267-274. https://doi.org/10.33994/kndise.2023.68.26

OSF. (2024). The role of state and local law enforcement in critical infrastructure protection. Retrieved from https://doi.org/10.17605/OSF.IO/MWNP9

Pettoello-Mantovani, C. (2024). Cybercrimes: An emerging category of offenses within the frame of the International Criminal Court jurisdiction. *International Journal of Law and Politics Studies*, *6*(2), 06-11. https://doi.org/10.32996/ijlps.2024.6.2.2

Raval, K. J., Jadav, N. K., Rathod, T., Tanwar, S., Vimal, V., & Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. *International Journal of Critical Infrastructure Protection*, *44*, 100647. https://doi.org/10.1016/j.ijcip.2023.100647

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

Sivek, S. C. (2024). The Data Analyst's Guide to AI. Retrieved from https://www.pecan.ai/blog/ai-for-data-analysts-guide/

Strmečki, S., & Pejaković-Đipić, S. (2023). Data protection, privacy, and security in the context of artificial intelligence and conventional

methods for law enforcement. *EU and Comparative Law Issues and Challenges Series, 7*, 571-589. https://doi.org/10.25234/eclic/27462

Vitanov, P. (2021). Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters. *European Parliament*. Retrieved from https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

## APPENDICES

## 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*)

**The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações**

***Contact:***
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

***Phone:*** +55(61)3107-2683/2688

***E-mail:*** getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET