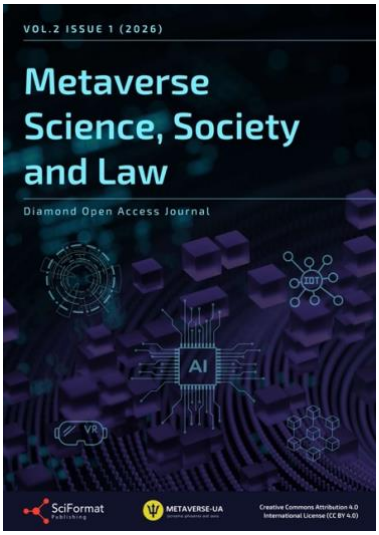

Metaverse Science, Society and Law

Vol. 2, Issue 1 (2026)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES
DOI	https://doi.org/10.69635/mssl.2026.2.1.35
RECEIVED	11 December 2025
ACCEPTED	17 March 2026
PUBLISHED	30 March 2026
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Oleksandr Nikitenko
Academician of the Academy of Administrative and Legal Sciences, Doctor of Juridical Sciences, Professor, Honoured Lawyer of Ukraine, Ukraine
ORCID ID: 0009-0001-6572-4072

Olena Kryzhanovska
Candidate of Economic Sciences, Ukraine

Illia Zhuravel
Postgraduate Researcher, Research Institute of Public Law, Ukraine
ORCID ID: 0009-0004-6486-6601

Volodymyr Zhuravel
Postgraduate Student of the Research Institute of Public Law, Ukraine

Bogdan Krymchanin
Third-Year Higher Education Student, State Tax University, Ukraine
ORCID ID: 0009-0003-4339-6658

ABSTRACT

The scientific study examines and substantiates, in accordance with the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" of 2017, No. 45, which defines the terms indicators of cyber threats, information on a cybersecurity incident, cybersecurity incident, cyberattack, cybersecurity, cyber threat, cyber defense, and others, while the terms "national security," "national interests," and "threats to national security" are used in this Law in the meaning defined by the Law of Ukraine "On the Fundamentals of National Security of Ukraine." The term "critical infrastructure object" is used in this Law in the meaning defined by the Law of Ukraine "On Critical Infrastructure." The rapid digitalization of social relations, the growing number of cyber threats, the spread of cybercrime, and the increasing complexity of digital attacks require law enforcement agencies to implement new technological solutions capable of ensuring the prompt detection, analysis, and neutralization of threats in cyberspace.

It has been established that artificial intelligence in law enforcement activity may be used for monitoring cyber incidents, detecting anomalous activity in information systems, analyzing large data sets, automating responses to certain events, classifying malicious software, countering phishing, and supporting digital investigations. This constitutes a generalization and logical development of the officially defined tasks of the cyber police, which include combating cybercrime, systematizing cyber incidents, informing the public, and interacting with foreign partners.

It has been proved that the combination of artificial intelligence and cybersecurity tools opens significant opportunities for carrying out reform processes in the field of law enforcement activity in Ukraine and for regulating the status of law enforcement agencies in the Constitution of Ukraine, while at the same time generating new regulatory and ethical risks associated with the protection of personal data, algorithmic bias, the opacity of automated decisions, liability for system errors, and the need for constant human oversight. It has been clarified that Ukraine still lacks a special comprehensive act that would separately regulate the application of artificial intelligence specifically for ensuring cybersecurity in the activities of law enforcement agencies; therefore, the relevant legal relations are currently governed by the provisions of the Law of Ukraine "On State Protection of Court Employees and Law Enforcement Officers" and the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine."

KEYWORDS

Artificial Intelligence, Cybersecurity, Law Enforcement Agencies, Cybercrime, Digital Technologies, Cyber Incidents, Information Security, Algorithmic Systems, Personal Data, Digital Investigations

CITATION

Oleksandr Nikitenko, Olena Kryzhanovska, Illia Zhuravel, Volodymyr Zhuravel, Bogdan Krymchanin. (2026) Artificial Intelligence and Cybersecurity in the Activities of Law Enforcement Agencies. *Metaverse Science, Society and Law*. Vol. 2, Issue 1. doi: 10.69635/mssl.2026.2.1.35

Introduction

The modern development of the information society is accompanied by the intensive transfer of a significant part of communications, managerial processes, financial transactions, and social interaction into the digital environment. Such transformation creates new opportunities for the state, business, and citizens, but at the same time forms a new range of threats associated with unauthorized interference in the operation of information systems, data theft, the dissemination of malicious software, phishing, cyber fraud, and the use of digital tools to commit other offenses [4].

Under such conditions, cybersecurity is becoming one of the key areas of ensuring national security, public order, and human rights. The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" directly defines the legal and organizational foundations for protecting the vital interests of the individual, society, and the state in cyberspace and thus grants cybersecurity the status of an independent area of state policy [4].

Within the system of entities responsible for ensuring public security and combating crime, an important place belongs to law enforcement agencies, primarily the National Police of Ukraine and specialized units operating in the field of prevention and counteraction to cybercrime in the sphere of ensuring the national security of Ukraine. The Law of Ukraine "On the National Police" defines the police as a central executive authority that serves society by safeguarding human rights and freedoms, combating crime, and maintaining public security and order [3].

A distinctive feature of the current stage is that law enforcement activity can no longer be effective without the use of intelligent digital tools. The increasing number of cyber incidents, the speed of attack propagation, and the large volume of digital evidence make traditional methods of information analysis insufficient. For this reason, artificial intelligence technologies are acquiring ever greater importance, as they are capable of processing large data sets, identifying complex patterns, and supporting decision-making in the field of cybersecurity [8].

The relevance of the topic is further reinforced by the fact that Ukraine is officially shaping a policy for the development of artificial intelligence through 2030, while the state is already developing institutional infrastructure for the implementation of AI solutions through the WINWIN AI Center of Excellence and related initiatives of the Ministry of Digital Transformation of Ukraine [12].

At the same time, the use of artificial intelligence in the field of cybersecurity of law enforcement agencies cannot be assessed solely from the standpoint of technical efficiency. It is associated with interference in the sphere of privacy, the processing of personal data, the risks of algorithmic error, the need for transparency of automated procedures, as well as the necessity of preserving human oversight over critically important decisions [10].

Despite the existence of a considerable number of scholarly works devoted to issues of artificial intelligence and cybersecurity in the activities of law enforcement agencies, this subject matter has still not received sufficiently complete and comprehensive coverage. Certain aspects thereof have become the subject of scientific research by such scholars as V. B. Averianov, O. M. Bandurka, V. M. Bevzenko, V. V. Halunko, I. P. Holosnichenko, O. Yu. Drozd, O. O. Kyrbiatiev, R. A. Kaliuzhnyi, V. K. Kolpakov, A. T. Komziuk, O. V. Kostenko, V. A. Lipkan, O. M. Muzychuk, O. I. Nikitenko, O. H. Predmestnikov, L. H. Chystokletov, S. H. Stetsenko, V. Ya. Tatsii, and others.

The purpose of this scientific study is to carry out a comprehensive analysis of the theoretical foundations of the relationship between artificial intelligence and cybersecurity in the activities of law enforcement agencies, as well as to characterize the practical aspects of the use of artificial intelligence for ensuring cybersecurity in the sphere of state security against internal and external threats

Part 1. Theoretical Foundations of the Relationship Between Artificial Intelligence and Cybersecurity in the Activities of Law Enforcement Agencies

Artificial intelligence, in its modern legal and technological understanding, should be regarded as a system or a set of systems capable, on the basis of data, of generating forecasts, recommendations, classifications, or other outputs that may influence decision-making. It is precisely this functional approach that underlies contemporary European regulation, in particular Regulation (EU) 2024/1689, known as the AI Act [8]. Cybersecurity should be defined not merely as a technical state of system protection, but as a complex of legal, organizational, informational, and technological measures aimed at protecting the individual, society, the state, and critical infrastructure in cyberspace. This broad approach is reflected in Ukrainian cybersecurity legislation [4].

The relationship between artificial intelligence and cybersecurity in the activities of law enforcement agencies is of a bilateral nature. On the one hand, artificial intelligence serves as an instrument for strengthening cybersecurity, since it enables more prompt detection of threats, analysis of digital traces, and response to cyber incidents. On the other hand, artificial intelligence systems themselves also require protection, as they may become objects of manipulation, data poisoning, model evasion, or unauthorized access [13].

For law enforcement activity, this relationship is of particular importance, as cyberspace is increasingly becoming an environment for the commission of crimes or a source of electronic evidence. The Council of Europe defines cybercrime as a substantial threat to human rights, democracy, the rule of law, international peace, and stability, and also indicates that practically any crime today may be connected with electronic evidence [7]. In this context, the role of law enforcement agencies lies not only in the investigation of already committed cybercrimes, but also in the prevention of attacks, recording of digital traces, international cooperation, analytical identification of criminal schemes, and development of preventive solutions. The officially defined tasks of the cyber police include the implementation of state policy in the field of combating cybercrime, the introduction of software tools for systematizing cyber incidents, responding to requests from foreign partners, and informing the public about cyber threats [11].

Theoretically, artificial intelligence in this area may be considered in three interrelated dimensions. The first dimension is analytical, where AI is used to identify anomalies, correlations, suspicious behavioral patterns, and for the rapid processing of large volumes of information. The second is managerial, where AI supports the prioritization of threats, allocation of resources, and formulation of recommendations for operational response. The third is legal, where AI acts as an object of regulation and requires the definition of the limits of permissible use, control procedures, and liability [8].

The key principle governing the use of artificial intelligence in the law enforcement sphere is legality. Any use of algorithmic tools must be based on a clearly defined legal basis, fall within the competence of the relevant authority, and be aimed at achieving a legitimate purpose. For law enforcement agencies, this requirement follows both from the constitutional model of state activity and from sector-specific legislation on the police, information, data protection, and cybersecurity [1].

The next principle is the priority of human rights. A law enforcement agency may not use artificial intelligence merely because it is technically convenient or fast. Any system must be applied with due regard for the right to privacy, the protection of personal data, the right to fair treatment, the prohibition of discrimination, and the possibility of appealing decisions that affect a person's legal status [10]. Of particular importance is the principle of human oversight. Modern international and European legal instruments proceed from the assumption that AI should not replace final human responsibility, especially in areas related to security, law and order, and human rights. A human being must retain the ability to verify an algorithmic conclusion, reject it, or require additional verification [10].

Transparency, accountability, and technical reliability are equally important. European approaches to trustworthy AI emphasize the need to ensure transparency, security, safety, proper data governance, non-discrimination, and responsibility for the consequences of the use of such systems [13]. Thus, the theoretical foundations of the relationship between artificial intelligence and cybersecurity in the activities of law enforcement agencies are formed at the intersection of administrative, information, criminal procedural, and international law, as well as modern technological approaches to the protection of the digital environment. In this field, artificial intelligence should be regarded not as an autonomous bearer of public authority, but as an auxiliary tool that enhances the state's capacity to respond to cyber threats, provided that clear legal limits and control are ensured [9].

Part 2. Practical Aspects of the Use of Artificial Intelligence for Ensuring Cybersecurity in the Activities of Law Enforcement Agencies

The practical significance of artificial intelligence for ensuring cybersecurity in the activities of law enforcement agencies lies primarily in the ability of such systems to process volumes of information that are difficult or impossible to analyze promptly solely by human effort. This concerns the implementation of the Law of Ukraine "On Operative-Investigative Activity" and the Law of Ukraine "On State Secrets," as well as the processing of events, network logs, incident reports, digital traces, malware samples, electronic correspondence, financial transactions, and data from open sources [11]. This statement constitutes an analytical conclusion derived from the officially defined tasks of the cyber police regarding the systematization of cyber incidents and the combating of cybercrime.

One of the most obvious areas of AI application is the detection of anomalous activity in information and communication systems. In the practice of ensuring cybersecurity, this may involve the automatic identification of unusual login attempts, suspicious changes in user behavior, atypical network requests, or activity characteristic of attacks. For law enforcement agencies, such systems are important both at the stage of оперативне response and at the stage of collecting information on potentially unlawful acts [4]. Another important area is the prioritization of cyber threats and the automated distribution of incident reports. Conditionally, such a system may filter out insignificant alerts, highlight critical events, recommend priority actions for the operator, and reduce the workload of personnel. It is precisely here that artificial intelligence acts not as a means of replacing human beings, but as a tool for increasing the speed of their work [13].

A practical area of AI use is also the analysis of phishing campaigns, fraudulent messages, malicious web resources, and other widespread instruments of cybercrime. Since the cyber police officially carry out advance public notification regarding the emergence of new cybercriminals and threats, AI systems may help identify typical patterns of deception, classify new schemes, and accelerate the preparation of warnings for citizens [11]. No less promising is the use of artificial intelligence in digital forensics. The subject matter of any legal science, like that of any independent scientific field, consists of the regularities that determine the development and change of specific groups of phenomena, facts, and relations. Criminalistics emerged and continues to develop as a science capable of assisting inquiry bodies, investigators, expert units, and the court in establishing the truth in judicial proceedings and in preventing crimes, including in the sphere of cybersecurity. During the investigation of cybercrimes, law enforcement officers encounter large volumes of electronic evidence: correspondence, files, access logs, device data, and network artifacts. Algorithmic systems are capable of accelerating preliminary sorting, the search for relevant fragments, and the identification of links between events and objects; however, the final assessment of such materials must remain with the authorized person and must be carried out in accordance with the requirements of procedural law [6].

In the field of detecting cybercrime, ensuring the national security of Ukraine, and international cooperation, artificial intelligence may also have considerable potential. At the same time, the effective implementation of such technologies requires not only technical solutions, but also a comprehensive strategic approach encompassing proper legislative regulation, human resources support, technological capacity, and financial resources [14]. The Budapest Convention on Cybercrime is regarded by the Council of Europe as the principal international framework for cooperation in the field of cybercrime and electronic evidence, while the officially defined tasks of the Ukrainian cyber police include responding to requests from foreign partners through channels of international cooperation [7]. Accordingly, algorithmic systems may facilitate the rapid analysis of requests, the grouping of similar incidents, and the preparation of materials for interstate communication.

At the same time, the practical application of AI in this sphere is associated with a number of significant risks. First, a system may make errors due to poor-quality or biased data. Second, excessive reliance on automated recommendations may lead to the so-called automation bias effect, where a person relies on the model's conclusion without sufficient verification. Third, AI systems themselves may be vulnerable to manipulation, data attacks, substitution of input information, or attempts to circumvent their logic [13]. A separate group of problems concerns privacy and the protection of personal data. In law enforcement activity, cybersecurity and artificial intelligence systems potentially operate with large volumes of personal information, technical identifiers, data on users' electronic behavior, digital profiles, and other sensitive information. Therefore, their use must be consistent with the requirements of legislation on information and personal data protection, as well as with international standards on privacy and data throughout the life cycle of AI systems [5].

An important practical requirement is also explainability. If a law enforcement agency uses AI for incident prioritization, the formation of suspicions, risk assessment, or the preparation of response recommendations, the official must understand, at least in general terms, why the system reached a particular conclusion. Otherwise, there arises a risk of non-transparent administration incompatible with the principles of accountability and control [9]. The practical implementation of such solutions also requires special training of personnel. The EU AI Act directly emphasizes AI literacy as a condition for the safe and proper use of intelligent systems. For law enforcement agencies, this means a need for specialists who understand not only the technical side of algorithms, but also the legal limits of their application, methods of verifying results, the risks of bias, and the requirements applicable to evidentiary information [8].

In view of the current state of Ukrainian legislation, it is advisable to gradually develop a special regulatory model for the use of AI in the field of cybersecurity of Ukrainian law enforcement agencies. Such a model should include the definition of permissible areas of application, the classification of high-risk systems, rules for testing and audit, requirements for data quality, procedures for human oversight, recording of system actions, the procedure for internal and external supervision, as well as mechanisms for administrative and judicial appeal against decisions adopted using AI [9].

Thus, the practical aspects of the use of artificial intelligence for the prevention, prophylaxis, detection, and ensuring of cybersecurity in the activities of law enforcement agencies demonstrate the significant potential of these technologies in the fields of monitoring, response, analytics, digital forensics, and international cooperation. However, the effectiveness of such use directly depends on the quality of legal regulation, the technical reliability of systems, data security, and the actual preservation of human oversight [10].

Conclusions

Thus, the relationship between artificial intelligence and cybersecurity in the activities of law enforcement agencies in the field of ensuring state security, as well as detecting and preventing cyber threats, is a natural consequence of the digital transformation of public administration and the increasing complexity of contemporary threats in cyberspace. The law enforcement system increasingly requires tools capable of rapidly detecting, processing, and interpreting large volumes of digital information, and artificial intelligence opens up new opportunities in this regard. The conducted analysis demonstrates that artificial intelligence can significantly strengthen the capacity of law enforcement agencies in the field of cybersecurity by increasing the speed of cyber incident detection, improving the analytical processing of data, optimizing responses to threats, assisting in digital investigations, and supporting international cooperation in cybercrime cases.

At the same time, the introduction of AI into this sphere also entails substantial risks associated with privacy, the protection of personal data, the technical vulnerability of models, the possibility of algorithmic error, the opacity of decisions, and the potential discriminatory nature of certain outcomes. For this reason, the effective use of artificial intelligence in the field of cybersecurity of law enforcement agencies is possible only provided that technological efficiency is combined with legal safeguards, ethical standards, and continuous human oversight.

At present, Ukraine lacks a separate special regulatory act that would comprehensively govern the use of artificial intelligence specifically for the cybersecurity needs of law enforcement agencies. The existing regulation is based on a combination of the provisions of legislation on the police, cybersecurity, information, personal data, criminal procedure, international mechanisms for combating cybercrime, and modern international approaches to the responsible use of AI. The prospects for the development of this area are associated with the formation of special administrative and legal mechanisms for the implementation of AI in the activities of law enforcement agencies, the introduction of procedures for risk assessment, system testing and auditing, the enhancement of AI literacy among personnel, as well as the harmonization of the national approach with European and international standards. Only under such conditions will artificial intelligence become not a source of new cyber risks, but an effective instrument for strengthening cybersecurity and enhancing trust in the law enforcement system.

REFERENCES

1. Constitution of Ukraine, No. 254k/96-VR. (1996, June 28). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. On information, No. 2657-XII. (1992, October 2). https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. On the National Police, No. 580-VIII. (2015, July 2). https://zakon.rada.gov.ua/laws/show/580-19#Text
4. On personal data protection, No. 2297-VI. (2010, June 1). https://zakon.rada.gov.ua/laws/show/2297-17#Text
5. On the basic principles of ensuring cybersecurity of Ukraine, No. 2163-VIII. (2017, October 5). https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Criminal Procedure Code of Ukraine, No. 4651-VI. (2012, April 13). https://zakon.rada.gov.ua/laws/show/4651-17#Text
7. Council of Europe. (2001, November 23). *Convention on cybercrime*. https://zakon.rada.gov.ua/laws/show/994_575#Text
8. European Parliament and Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
9. Council of Europe. (n.d.). *The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence
10. UNESCO. (n.d.). *Recommendation on the ethics of artificial intelligence*. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
11. Cyberpolice Department of the National Police of Ukraine. (n.d.). *Cyberpolice: Official website of the Cyberpolice Department of the National Police of Ukraine*. https://cyberpolice.gov.ua/
12. Ministry of Digital Transformation of Ukraine. (2025, June 26). *The Ministry of Digital Transformation is shaping an AI strategy—Join the survey and influence the future of AI in Ukraine*. https://thedigital.gov.ua/news/technologies/mintsifra-formue-strategiyu-z-shi-doluchaytesya-do-opituvannya-i-vplivayte-na-maybutne-shi-v-ukraini
13. European Commission. (n.d.). *Ethics guidelines for trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
14. Kostenko, O. V. (2022). Analysis of national strategies for the development of artificial intelligence. *Information and Law, 2*(41), 58–69. https://doi.org/10.37750/2616-6798.2022.2(41).270365