European Research Studies Journal
Volume XXVII, Issue 3, 2024

pp. 962-973

Utilization of Artificial Intelligence in Security Management within an Organization

Submitted 10/09/24, 1st revision 25/09/24, 2nd revision 01/10/24, accepted 15/10/24

Marian Kopczewski[1], Jolanta Wojtowicz-Żygadło[2], Sławomir Żurawski[3], Sylwester Pietrzyk[4]

Abstract:

Purpose: *The purpose of the article is to analyse the role of artificial intelligence (AI) in organizational security management, including its impact on improving protection effectiveness and identifying challenges associated with implementing these technologies. The first part of the article addresses contemporary challenges in organizational security management and the essence of AI in modern management. The second part discusses specific applications of AI, including the use of machine learning, natural language processing (NLP), and image recognition algorithms that support both digital and physical security. The third part analyses the challenges associated with implementing AI.*
Design/Methodology/Approach: *The research problem is formulated as a question: Does the application of artificial intelligence in security management contribute to a significant reduction in risk and improvement in protection efficiency? The research hypothesis assumes that the use of AI increases the effectiveness of protective actions through process automation, threat prediction, and faster response, but it also involves challenges such as personal data protection and high system complexity. The article employs theoretical methods, including literature analysis, industry reports, and international research findings. This approach provides a comprehensive view of security management topics utilizing AI.*
Findings: *The conclusions indicate that artificial intelligence has the potential to revolutionize security management by offering effective predictive and analytical tools. However, its full utilization requires addressing issues related to privacy protection, decision-making transparency by algorithms, and the availability of specialists. Further research in this area is necessary for AI technologies to responsibly and sustainably support organizations in ensuring safety.*
Practical implications: *AI technologies, such as machine learning and real-time data analysis, facilitate faster anomaly detection and provide more accurate risk assessments. This enables organizations to better prepare for cyber threats and other forms of operational*

[1]*Military University of Land Forces in Wrocław, Poland, ORCID:0000 -0002-0402-0477 marian.kopczewski@interia.pl;*
[2]*State Academy of Applied Sciences in Jarosław, Poland, ORCID:0000-0001-5688-3998; jolanta.wojtowicz-zygadlo@pansjar.edu.pl;*
[3]*State Academy of Applied Sciences in Chełm, ORCID:0000-0001-9527-3391, slawomir.zurawski@onet.pl;*
[4]*Warsaw Management University, Poland, ORCID:0000-0001-7697-0853, spietrzyk16@gmail.com;*

risk. Simultaneously, advanced AI systems integrate with existing security tools, enhancing their effectiveness without requiring a complete overhaul of technological infrastructure.
Originality/value: *Artificial intelligence has the potential to revolutionize security management in organizations by offering more efficient, scalable, and precise solutions. However, its full utilization requires not only appropriate technological implementation but also an understanding of emerging threats and the development of suitable risk management strategies. Further research and investment in this area are crucial to ensure that AI development strengthens security in a sustainable and responsible manner.*

Keywords: *Security, management, artificial intelligence, organization, new technologies*.

JEL codes: *M12, L31*.

Paper type: *Research article.*

1. Introduction

In an era of dynamic technological changes, artificial intelligence (AI) is becoming one of the key factors influencing how modern organizations operate. This technology transcends the boundaries of traditional analytical tools, offering new possibilities in areas such as data analysis, process automation, and decision support. Organizational security management, which is one of the most important aspects of the functioning of companies and institutions, is currently undergoing significant transformations due to the implementation of AI-based solutions. In the context of increasing threats such as cyberattacks, internal fraud, and rising systemic risk, the role of artificial intelligence becomes invaluable.

Managing organizational security now requires a multidimensional approach that encompasses both technological and organizational aspects. Traditional protective tools, such as firewalls and intrusion detection systems, are increasingly proving insufficient in the face of the complexity of modern threats. AI introduces new capabilities, such as self-learning systems that analyse vast amounts of data in real time, identify unusual patterns of behaviour, and suggest appropriate remedial measures. The implementation of such solutions can not only improve protection effectiveness but also contribute to optimizing costs associated with security.

According to reports from McKinsey & Company, organizations that effectively utilize AI report an average 20% higher efficiency in risk management compared to those relying solely on traditional methods. Moreover, Gartner's research shows that 45% of companies plan to increase investments in AI supporting security over the next three years, indicating a growing awareness of the importance of this technology. The aim of this article is to provide a comprehensive discussion on the role of artificial intelligence in security management within organizations.

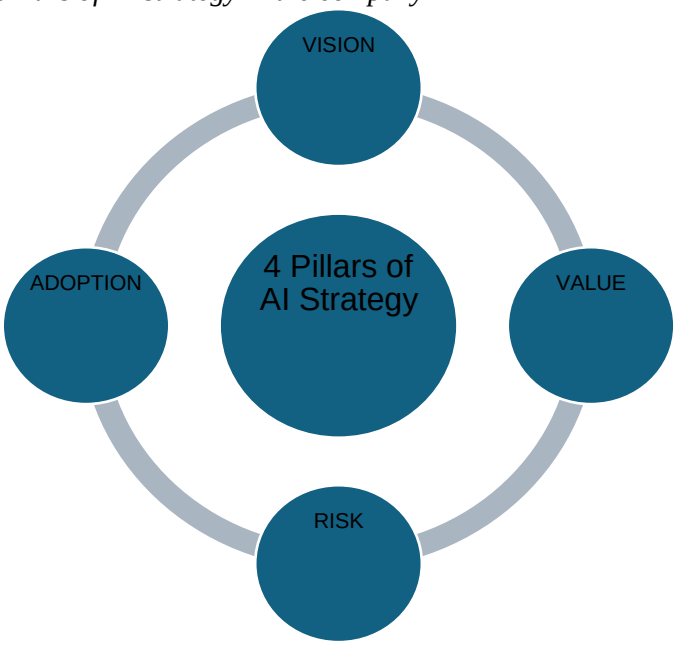
The article consists of three main parts: the first analyses contemporary challenges in security management; the second discusses key applications of AI in this area; and the third presents future directions for the development of AI technology in the context of risk management and data protection. The publication is based on subject literature, statistical data, and international research findings, offering a comprehensive view of this dynamically evolving topic.

2. The Role of Artificial Intelligence in Modern Security Management

Artificial intelligence refers to the ability of computer systems to perform tasks traditionally requiring human intelligence, such as pattern recognition, decision-making, and data analysis (Brynjolfsson and McAfee, 2017, pp. 45-47).

AI is gaining increasing importance in security management, becoming one of the key tools utilized by organizations across various fields (Nowicka *et al.*, 2024, p. 461). AI enables systems to detect threats, predict incidents, and take preventive actions, allowing organizations to monitor resources more effectively and respond to potential dangers. According to Gartner, a company specializing in strategic technology utilization, enhancing the following pillars of their AI strategy is essential for gaining a greater impact on artificial intelligence.

Figure 1. *Four key pillars of AI strategy in the company*



Source: *Gartner: Building a value-based artificial intelligence strategy for your company.*

Examples of the application of artificial intelligence in security management include both areas related to cybersecurity and physical protection (Chrząszcz *et al.*, 2024, p.

771). In the field of cybersecurity, AI enables the analysis of network traffic, allowing for the rapid detection of anomalies indicating possible attacks, such as intrusions or data theft attempts. By utilizing advanced artificial intelligence algorithms, monitoring systems can identify subtle irregularities in the network that may go unnoticed by traditional signature-based or rule-based detection methods.

Conversely, in the context of physical security, AI has been applied in video surveillance systems that use facial recognition or behaviour analysis algorithms, enabling automatic detection of unauthorized individuals or suspicious activities. This technology significantly enhances the effectiveness of monitoring public spaces such as airports, shopping centres, or industrial facilities. AI is also used in access control systems, where it enables automatic recognition of individuals authorized to enter specific areas based on biometric data such as fingerprints or facial recognition.

The use of artificial intelligence in organizational security has many advantages, the most important being increased efficiency of protective actions. AI allows for the automation of many processes related to monitoring and responding to threats, which not only shortens response times to incidents but also enables more precise identification of potential threats. An example of this could be automatically blocking access to IT systems upon detecting suspicious activities, such as ransomware or phishing attempts.

Artificial intelligence also allows for threat prediction, which is possible through the analysis of large datasets such as historical data, network traffic, or behaviour patterns. Based on this information, AI systems can indicate which areas of the organization are most vulnerable to attacks and where additional precautions should be taken.

The benefits of implementing AI in security management are particularly evident for organizations that must protect both digital data and physical resources. Modern challenges associated with the increasing number of cyber threats, such as DDoS attacks, malware, or ransomware, require advanced tools for detection and prevention. AI systems not only allow for faster detection of such threats but also enable automatic implementation of appropriate countermeasures, such as isolating compromised network segments or blocking malicious software.

In terms of physical protection as well, AI supports traditional monitoring methods by enabling the detection of suspicious behaviours in crowds or unauthorized access to protected areas. Through advanced real-time image analysis, AI-based video monitoring systems can identify threats faster than the human eye, allowing for immediate responses from security personnel.

One of the most significant advantages of AI in security management is its ability to learn and adapt to a changing threat environment (Przegalińska-Skierkowska, 2023).

Machine learning algorithms enable AI systems to continuously improve their capabilities in pattern recognition and anomaly detection. As new data is collected, these systems become increasingly accurate at identifying new types of threats and predicting their occurrence. Consequently, AI is a key element in developing proactive security strategies that anticipate potential attacks before they occur.

From an organizational perspective, implementing artificial intelligence in security also brings benefits related to cost reduction and process optimization. Automating tasks such as data analysis or network monitoring reduces the workload on security personnel, allowing them to focus on more complex tasks. Furthermore, AI-based systems offer greater scalability, which is particularly important for large organizations that must manage vast amounts of data and resources. AI enables effective real-time monitoring and management of security even within distributed infrastructures.

Despite numerous benefits, the application of artificial intelligence in security management also presents certain challenges. One major issue is data privacy concerns, especially regarding the use of facial recognition systems or behaviour analysis. This necessitates compliance with relevant legal regulations such as the General Data Protection Regulation (GDPR) in the European Union, which imposes restrictions on collecting and storing personal data. Additionally, AI systems may be vulnerable to attacks such as input data manipulation, potentially leading to erroneous decisions or inappropriate responses to threats.

In the future, artificial intelligence in security management will continue to evolve, and organizations will need to adapt their strategies to new technologies and challenges. As cyber threats grow increasingly complex and the need for security in an ever-more automated world intensifies, the role of AI in protecting digital and physical resources will become increasingly significant.

The integration of AI with other technologies such as the Internet of Things (IoT), robotics, or blockchain will open new possibilities in security management by enabling the creation of more complex and effective protection systems (Ogórek and Zaskórski, 2018, p. 202).

In summary, artificial intelligence plays a crucial role in modern security management by providing organizations with tools for detecting threats, predicting incidents, and automatically responding to them. With AI, it is possible not only to enhance the efficiency of protective actions but also to develop more advanced preventive strategies that outpace threats.

Although this technology presents certain challenges, its future in security management looks promising, offering limitless opportunities for protecting digital and physical resources.

3. Artificial Intelligence Tools Supporting Security Management - Technologies and Solutions Used in Practice

Artificial intelligence (AI) tools are playing an increasingly important role in modern security management, assisting organizations in identifying, analysing, and responding to threats. Among these tools, machine learning algorithms are crucial as they enable the analysis of vast datasets to detect risk patterns and predict potential incidents (Ciekanowski *et al.*, 2024, p. 463). With the ability to process and analyse data in real-time, machine learning-based systems can identify anomalies or threats that may be overlooked by traditional methods.

An example of a system utilizing machine learning in security management is Security Information and Event Management (SIEM) software, which collects data from various organizational systems such as identity management systems, firewalls, endpoints, and applications. SIEM allows for the analysis of this data for potential threats, automatically identifying and alerting security incidents in real-time. This capability enables organizations to respond more quickly to cyberattacks, thereby reducing the risk of significant losses or data breaches (Resilia, 2023). SIEM software also supports audit and compliance processes by generating reports and monitoring adherence to established standards and regulations.

In the context of advanced AI technologies, neural networks represent another essential element used in security management. Artificial neural networks are algorithms that simulate the way information is processed in the human brain, making them particularly effective in analysing large datasets and recognizing complex patterns. Their ability to learn from examples allows neural networks to automatically identify anomalies that may indicate cyberattacks, such as system intrusions or malware spread.

These technologies are also applied in crisis situations like natural disasters or infrastructure failures, where real-time data analysis is critical for making swift and accurate decisions. For instance, a crisis management system might predict possible scenarios of power grid failures or water supply disruptions by analysing data from sensors distributed throughout the infrastructure. This capability enables organizations responsible for crisis management to better prepare for potential threats, minimizing losses and impacts from disasters.

Another AI technology applied in security management is natural language processing (NLP). NLP is a branch of artificial intelligence that enables computers to understand and analyse human language (Maciąg, 2024, p. 64). These technologies are utilized by organizations to analyse internal communications such as emails, documents, or messages in chat applications to detect potential threats including phishing attempts, fraud, or misinformation manipulation. NLP systems examine message content to identify irregularities in language structure, such as suspicious links or email addresses, as well as keywords that may suggest data theft

attempts or social engineering attacks. This enables organizations to effectively respond to such threats before incidents occur, such as losing confidential information or compromising information system integrity.

NLP technologies are also employed in analysing external communications, for example in monitoring social media or online forums where signals regarding potential threats related to an organization's reputation or resources can be detected. Automated analysis of large text datasets allows for rapid responses to crisis situations like the spread of false information or unauthorized publication of confidential data.

Another advanced solution supporting security management is the use of image and video recognition technology. AI algorithms can analyse images from surveillance cameras to detect unauthorized individuals, suspicious behaviours, or other undesirable situations. These technologies are applied in both physical spaces and cybersecurity contexts where image analysis can assist in recognizing attempts at system breaches or unauthorized access to resources.

Facial recognition is one of the most advanced methods used in monitoring systems that allows for identifying individuals in crowds and checking whether they are listed in authorized user databases (Lewandowski, 2021, p. 85). Such technologies are employed in airports, shopping centres, stadiums, and other public places where high security is required.

The integration of various AI technologies such as machine learning, neural networks, NLP, and image recognition creates comprehensive solutions that effectively support security management. With these tools, organizations can monitor and protect their resources in real-time while effectively responding to threats. Moreover, these technologies not only enhance the efficiency of protective actions but also allow for the automation of many processes, significantly reducing the risk of human errors and speeding up response times.

However, like any new technology, the use of artificial intelligence comes with certain challenges such as ensuring data privacy, resilience against hacking attacks, and managing system complexity. Nevertheless, with technological advancements, AI tools in security management are becoming increasingly effective and represent a vital component in building modern and secure organizations.

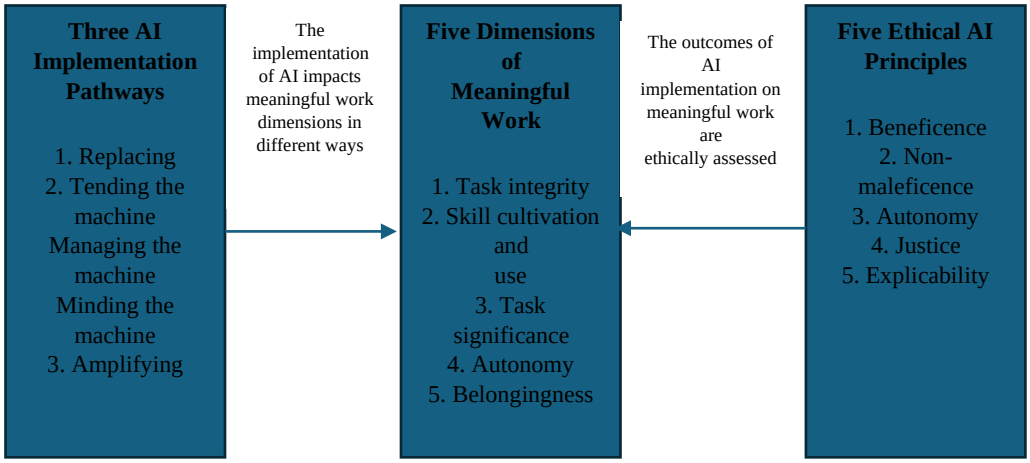
4. Challenges and Perspectives on the Development of AI in Security Management - Ethical and Legal Issues

The implementation of artificial intelligence (AI) in security management involves a number of challenges that organizations must overcome to fully leverage the potential of this technology. One of the key issues is ensuring compliance with legal regulations, particularly in the context of personal data protection. The use of

artificial intelligence to analyse vast datasets, including personal data, raises questions about privacy protection and adherence to regulations such as the General Data Protection Regulation (GDPR) in the European Union. The introduction of technologies such as facial recognition systems or communication monitoring can lead to situations where individuals' privacy is at risk.

Organizations must implement appropriate data protection mechanisms to ensure compliance with legal requirements while minimizing the risk of infringing on users' privacy. The GDPR, with its requirements for transparency, accountability, and consent for data processing, presents challenges for companies regarding the storage, processing, and securing of data in a manner that does not violate the rights of individuals whose data is being analysed. A conceptual overview of the application of artificial intelligence is presented below.

Figure. 2 *Overview of conceptual framework*



Source: *S. Bankins, P. Formosa, (2023).*

In the context of privacy protection, the issue of transparency in decisions made by artificial intelligence systems also arises. AI, relying on algorithms that learn from data, often makes decisions that can be difficult for humans to understand, especially in more complex systems based on neural networks or other advanced technologies. Such "black boxes" pose a significant challenge regarding accountability for the decisions made. If artificial intelligence algorithms make a mistake—such as in the case of a faulty threat analysis—assigning responsibility for the consequences of that decision can be challenging.

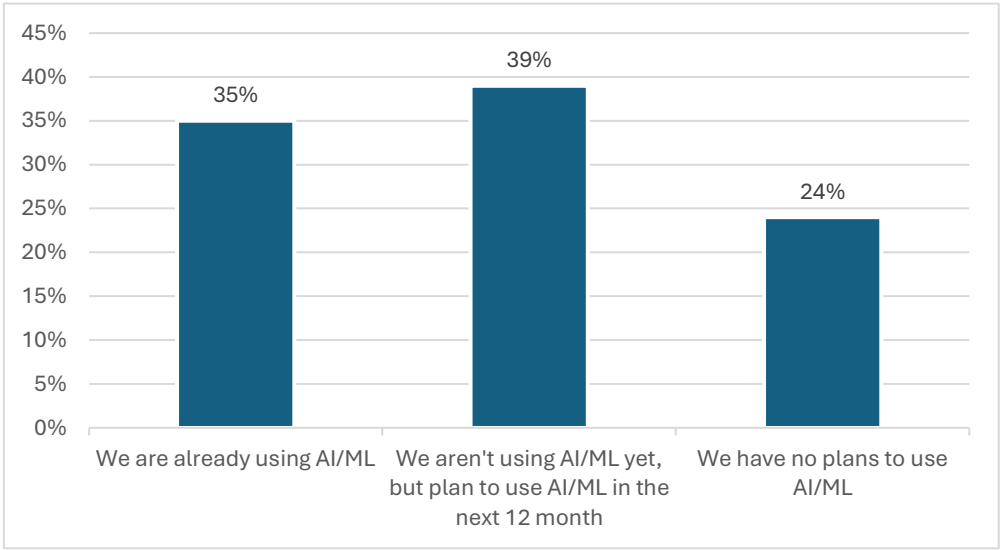
This raises questions about who is accountable for decisions made by AI systems: is it the creator of the algorithm, the organization implementing the technology, or perhaps the system itself that operates based on these algorithms? Additionally, errors in recognition or analysis of incomplete data can lead to false alarms or

unidentified threats, resulting in undesirable consequences such as unnecessary system shutdowns or incorrect preventive actions. Addressing these challenges requires implementing algorithmic transparency and auditing procedures that allow for monitoring and evaluation of these systems' effectiveness.

Another challenge associated with implementing AI in security management is the high costs related to deploying and maintaining these technologies. Although the potential benefits from automating processes and improving security management effectiveness are significant, for many organizations, initial costs can be a substantial barrier. Investments in artificial intelligence, including hardware purchases, software acquisition, and hiring specialists, can be very expensive, particularly for smaller companies that do not have large technology budgets.

Furthermore, the ongoing need to maintain and update AI systems incurs additional operational costs. There is also a shortage of qualified specialists capable of managing complex AI systems and integrating them with existing organizational infrastructure. Industry reports indicate that only a small percentage of organizations worldwide fully integrate AI systems with their existing management structures. The limited availability of skilled professionals often leads companies to outsource the development of such systems or delay technology implementation, which can impact their competitiveness in the market. A Forrester Research Report presented the percentage of companies using AI or planning to use it within the next twelve months; results are detailed below.

Figure 3. *The number of companies using AI or planning to use it in the next twelve months*



Source: *Forrester Research Report (2023).*

Despite these challenges, the prospects for the development of artificial intelligence in security management are promising. The strategic perspective of humanity must take into account the emergence of artificial intelligence and also consider the scenario in which it surpasses a critical point, achieving a significant advantage over humans in all areas of knowledge (Grochmalski, 2019, p. 111).

In the coming years, AI technologies will become increasingly integrated with other modern technological solutions, such as the Internet of Things (IoT) and blockchain. This integration will enable even greater automation of processes and improve the efficiency of security management systems. The combination of AI with IoT will allow for more precise monitoring of devices and infrastructure, detecting threats before they occur. Meanwhile, blockchain can enhance data security by ensuring its integrity and resistance to unauthorized changes. It is anticipated that as technology advances, new solutions will emerge that are even more advanced, effective, and flexible in responding to dynamically changing threats.

Artificial intelligence, although already widely used in security management, still faces numerous challenges that must be addressed for it to fully realize its potential. Ethical issues such as ensuring privacy and transparency in decision-making, along with legal concerns like compliance with data protection regulations, require special attention.

Additionally, high implementation costs and a lack of qualified specialists can pose significant barriers for smaller organizations. Nevertheless, the development of AI and its integration with other technologies offers hope for a future where security management becomes more efficient, automated, and secure. In light of increasing threats—both digital and physical—the advancement of artificial intelligence in security management is becoming not only an opportunity but also a necessity.

5. Conclusions

Artificial intelligence (AI) is playing an increasingly significant role in organizational security management, providing tools that enhance the efficiency of threat identification, risk management, and incident response. The use of AI allows for the automation of security processes, reducing reliance on manual actions and minimizing risks associated with human errors. Additionally, advanced predictive algorithms enable the forecasting of potential threats, thereby increasing the proactivity of organizations in protecting their assets.

AI technologies, such as machine learning and real-time data analysis, support faster anomaly detection and provide more accurate risk assessments. This capability allows organizations to better prepare for cyber threats and other forms of operational risk. At the same time, advanced AI systems integrate with existing security tools, enhancing their effectiveness without necessitating a complete overhaul of technological infrastructure.

Despite the many benefits of implementing AI in security management, further research is essential on several key aspects. One challenge is ensuring that algorithms are transparent and free from biases that could lead to unfair or suboptimal decisions. Another critical research area involves securing AI systems against attacks, such as manipulation of training data or control over algorithms. As organizations become increasingly dependent on AI, they must also invest in developing their employees' skills to understand both the capabilities and limitations of these technologies.

In summary, artificial intelligence has the potential to revolutionize security management within organizations by offering more effective, scalable, and precise solutions. However, fully realizing this potential requires not only appropriate technological implementation but also an understanding of emerging threats and the development of suitable risk management strategies. Continued research and investment in this area are crucial to ensure that AI development contributes to enhancing security in a sustainable and responsible manner.

References:

Accenture. 2024. How is AI shaping the cybersecurity strategies of tomorrow? https://www.accenture.com/us-en/blogs/security/how-ai-shaping-cybersecurity-strategies.

Artificial intelligence (AI) cybersecurity. https://www.ibm.com/ai-cybersecurity?.

Bankins, S., Formosa, P. 2023. The Ethical Implications of Artificial Intelligence (AI) for Meaningful Work. Journal of Business Ethics, 185, pp. 725-740.

Brynjolfsson, E., McAfee, A. 2017. Machine, Platform, Crowd. WW Norton & Company, 45-67.

Chrząszcz, A., Ciekanowski, M., Żurawski, S., Załoga, W., Pietrzyk, S. 2024. Managing Organizational Security in the Context of Global Challenges. European Research Studies Journal, Volume XXVII, Issue 3, pp. 765-777.

Ciekanowski, Z., Nowicka, J., Czternastek, M., Żurawski, S., Mikosik, P. 2024. How Cybersecurity Shapes Effective Organizational, European Research Studies Journal, Volume XXVII, Issue 2, pp. 454-464.

Deloitte Insights. 2023.

EU Artificial Intelligence Act. https://artificialintelligenceact.eu/ai-act-explorer/.

Forrester Research Report. 2023.

Gartner. 2023. What's New in Artificial Intelligence from the 2023 Gartner Hype Cycle. https://www.gartner.com/en/articles/what-s-new-in-artificial-intelligence-from-the-2023-gartner-hype-cycle.

Grochmalski, P. 2019. Nowy paradygmat bezpieczeństwa a AI. Cybersecurity and Law, vol. 1(1), 93-113.

Lewandowski, L. 2021. Alternatywne narzędzia zdalnej identyfikacji. Przegląd Bezpieczeństwa Wewnętrznego, nr 25, 85-101.

Maciąg, R. 2024. Large Language Models Technology as a Center of Knowledge Flows in the Organization: Epistemic Management. In: Zarządzanie organizacją w społeczeństwie informacyjnym. Problemy Szanse Wyzwania Perspektywa interdyscyplinarna, red. Wójcik, M., Berkowicz, A. Biblioteka Jagielońska, Kraków.

Nowicka, J., Ciekanowski, Z., Kudins, J., Dabrowski, P.J. 2024. Managing Organizational Security in the Era of Digital Transformation. European Research Studies Journal, Volume XXVII, Issue 3, pp. 460-471.

McKinsey & Company. 2017. Rewolucja AI. Jak sztuczna inteligencja zmieni biznes w Polsce.

Ogórek, M., Zaskórski, P. 2018. Internet rzeczy w integracji procesów zarządzania kryzysowego, Zeszyty Naukowe Politechniki Poznańskiej, nr 76, 199-215.

Polskie Towarzystwo Informatyczne. 2023. Aktualne wyzwania sztucznej inteligencji. https://pti.org.pl/awsi/.

Przegalińska-Skierkowska, A. 2023. AI w strategii: rewolucja sztucznej inteligencji w zarządzaniu. Wydawnictwo MT Biznes.

Raport PwC Global AI Jobs Barometer. 2024.

Statista. 2023. Global AI market size 2030.