Dydaktyka Informatyki 20(2025)
ISSN 2083-3156; e-ISSN 2543-9847
DOI: 10.15584/di.2025.20.5
https://www.journals.ur.edu.pl/di

Uniwersytet Rzeszowski

Agnieszka MOLGA[1], **Jacek WOŁOSZYN**[2]

[1] *ORCID: 0000-0002-0857-5111. Dr, Uniwersytet Radomski, Wydział Transportu, Elektrotechniki i Informatyki, Katedra Informatyki, ul. Malczewskiego 29, 26-600 Radom, e-mail: agnieszka19216@wp.pl*

[2] *ORCID: 0000-0003-4340-9853. Dr inż., Uniwersytet Radomski, Wydział Informatyki i Matematyki, Katedra Informatyki, ul. Malczewskiego 20A, 26-600 Radom, e-mail: jacek.woloszyn@uthrad.pl*

data złożenia tekstu do Redakcji DI: 26.04.2025; data wstępnej oceny artykułu: 5.05.2025

AI AND CYBERSECURITY – WILL AI BECOME THE SHIELD OF THE NETWORK?

SZTUCZNA INTELIGENCJA A CYBERBEZPIECZEŃSTWO – CZY AI STANIE SIĘ TARCZĄ SIECI?

Keywords: artificial intelligence, machine learning, neural networks, robotics, expert systems.

Słowa kluczowe: sztuczna inteligencja, uczenie maszynowe, sieci neuronowe, robotyka, systemy ekspertowe.

Abstract

The article explores the growing importance of artificial intelligence (AI) in the field of cybersecurity and how AI technologies can enhance network defense against cyber threats. It highlights key areas where AI is already being applied, such as threat detection and analysis, incident response automation, and strengthening security systems through machine learning. The authors emphasize that AI enables rapid and efficient processing of vast amounts of data-essential for real-time network traffic monitoring and threat analysis. With the use of machine learning techniques, it becomes possible to identify patterns that may indicate potential attacks, allowing for proactive protective measures.

Streszczenie

Artykuł omawia rosnącą rolę sztucznej inteligencji (AI) w obszarze cyberbezpieczeństwa oraz przedstawia, w jaki sposób technologie AI mogą wspierać ochronę sieci przed zagrożeniami cybernetycznymi. Omówiono główne zastosowania AI, takie jak wykrywanie i analiza zagrożeń, automatyzacja reakcji na incydenty oraz wzmacnianie systemów ochrony z wykorzystaniem ucze-

nia maszynowego. Zwrócono uwagę na to, że AI umożliwia błyskawiczne przetwarzanie ogromnych ilości danych – kluczowe w kontekście monitorowania ruchu sieciowego i analizy zagrożeń w czasie rzeczywistym. Dzięki algorytmom uczenia maszynowego możliwe jest rozpoznawanie schematów mogących świadczyć o potencjalnych atakach, co pozwala na szybsze i skuteczniejsze działania zapobiegawcze.

1. What is artificial intelligence?

Artificial Intelligence (AI) is a field of computer science focused on creating systems capable of making decisions and performing tasks that traditionally required human intelligence and reasoning. While not long ago it was mostly associated with science fiction, today AI is a rapidly evolving area with a real impact on many aspects of everyday life.

The development of AI evokes mixed reactions. On one hand, these technologies can significantly accelerate and streamline the execution of numerous tasks. On the other hand, concerns arise about job automation and the potential disappearance of certain professions.[1] At the same time, there is a growing belief that skillful implementation of AI can lead to the creation of entirely new careers and professional paths. Even now, AI-based solutions are opening up previously unimaginable possibilities–especially in critical areas such as cybersecurity.[2]

As a set of advanced algorithms and techniques, artificial intelligence enables computers to learn and make decisions based on data. In the context of digital security, this represents immense value–AI can analyze vast amounts of information, identify unusual patterns and potential threats, and respond to them in real time. Thanks to its capacity for continuous improvement[3], AI systems are becoming increasingly effective, enhancing the accuracy and efficiency of network protection. Artificial intelligence is not just a tool for automating processes, but a key component of future network defense strategies, offering new ways to detect and respond to cyber threats. It is a dynamic field of research and innovation with the potential to transform many aspects of our professional and personal lives. Artificial Intelligence (AI) refers to technologies capable of understanding, learning, and acting based on acquired and processed information. Today, AI operates on three levels[4]:

[1] M. Raj, & A. Sharma, *Artificial Intelligence and Cybersecurity: Enhancing Network Defense*, Springer 2021.

[2] P. Nguyen, & K. Lee, *Machine Learning for Cybersecurity: A Practical Guide*, Academic Press 2022.

[3] W. Bieliński, & J. Kowalski, *Sztuczna inteligencja w bezpieczeństwie komputerowym: wyzwania i możliwości*, Wyd. Naukowe PWN 2020.

[4] M. Kowalski, *Automatyzacja procesów ochrony w cyberbezpieczeństwie przy wykorzystaniu AI*, Wyd. Wydziału Informatyki Politechniki Warszawskiej 2023.

1. Assisted Intelligence – Already widely used, it helps individuals and organizations streamline their actions and processes.

2. Augmented Intelligence – Currently being implemented, it enables the performance of tasks that were previously beyond human or technological capabilities.

3. Autonomous Intelligence – A technology of the future, it envisions the creation of systems capable of making decisions and acting independently, without human involvement.

The main areas of artificial intelligence application include:[5]

- Deep Learning: This is an advanced form of machine learning based on the operation of neural networks–structures modeled after the human brain. Deep learning enables the processing of vast datasets and the automatic detection of patterns and key features, which is used in image recognition, classification, and object detection.
- Natural Language Processing (NLP): This branch of AI allows computers to understand, interpret, and generate human language in a way that is both understandable and useful. NLP is applied in machine translation tools, sentiment analysis, and voice assistants, facilitating human interaction with technology.
- Machine Learning: Focuses on developing models that can learn from data and experience. Rather than being explicitly programmed to perform specific tasks, algorithms learn from examples and are capable of predicting outcomes, making decisions, or recognizing patterns without manually coding each step.

2. The Importance and Application of Artificial Intelligence in the Field of Cybersecurity

The ENISA report titled *Artificial Intelligence Cybersecurity Challenges. Threat Landscape for Artificial Intelligence* discusses the connections between artificial intelligence and cybersecurity on several key levels:[6]

- the protection of AI systems themselves,
- the use of AI to enhance digital security,
- and the potentially harmful applications of AI by cybercriminals.

[5] M.S., Hossain, & G. Muhammad, *Artificial Intelligence for Cybersecurity: Foundations, Techniques, and Applications*, CRC Press 2021.

[6] ENISA, *Artificial Intelligence Cybersecurity Challenges: Threat Landscape for Artificial Intelligence*. European Union Agency for Cybersecurity 2020. Retrieved from https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges (dostęp: 11.02.2024).

In the context of network security, AI plays an increasingly important role–supporting data analysis, threat detection, and the automation of defense mechanisms.[7] With its ability to process vast amounts of information in a short time, artificial intelligence is becoming an essential tool in combating modern cyberattacks. AI-powered behavioral analytics enable the rapid identification of unusual user activities and immediate responses to potential incidents.[8] Neural networks used for this purpose effectively recognize patterns typical of cyber-criminal operations. One practical example of AI application in cybersecurity is Next Generation Antivirus (NGAV) software. Unlike traditional solutions, NGAV does not rely solely on signature databases but instead uses machine learning and artificial intelligence to detect previously unknown threats. Thanks to their adaptability and self-improvement capabilities, NGAV solutions can effectively defend against even the most advanced forms of cyberattacks, responding to them in real time.

3. Intelligent Systems in Cybersecurity

In the face of rapid technological change, cybersecurity is becoming one of the most critical challenges for businesses, institutions, and individual users alike. As digital solutions evolve, cyber threats are growing in complexity and becoming increasingly difficult to detect. Cybercriminals continuously refine their techniques, which drives security experts to constantly search for new tools to effectively detect, neutralize, and mitigate the effects of attacks.[9] One of the most promising approaches to combating this phenomenon is the use of artificial intelligence (AI).

In recent years, the cybersecurity sector has undergone a significant transformation, largely due to the implementation of AI-based solutions. The automation of processes, improved threat detection capabilities, and the development of defense tools have made AI an essential part of security strategies. At the same time, Managed Security Service Providers (MSSPs) are faced with increasingly sophisticated and diverse attacks.

AI not only accelerates analysis and response processes but also enables organizations to manage digital transformation more effectively. On the other

[7] M. Aldosari, *AI-driven Security Systems: Safeguarding Networks in the Age of Artificial Intelligence*, Taylor & Francis 2020.

[8] K. Zieliński, *Bezpieczeństwo cyfrowe w erze sztucznej inteligencji*, Wyd. Akademickie Dialog 2022.

[9] M. Sienkiewicz, *Sztuczna inteligencja w cyberbezpieczeństwie: nowoczesne rozwiązania ochrony sieci*, Wyd. Helion 2019.

hand, cybercriminals are also leveraging the power of AI, developing automated, multi-vector attacks capable of evading traditional detection mechanisms.[10]

With the growing number of network-connected devices, security systems are overwhelmed by vast volumes of alerts. By utilizing artificial intelligence, security service providers can analyze data more quickly, identify potential threats, and develop effective defense strategies. AI significantly reduces response times–from days or weeks to just a few minutes.

That is why it is crucial for companies to quickly familiarize themselves with the capabilities offered by artificial intelligence. Only then will they be able to fully leverage its potential to protect against the growing spectrum of digital threats.

Providing cybersecurity is inherently tied to risk analysis. To achieve this, the latest technologies must be implemented, including those based on artificial intelligence.[11] Rapid technological development has significantly accelerated this process. According to the NASK report "Cybersecurity AI. AI in Cybersecurity", AI tools are used both for defense and for carrying out cyberattacks. AI works for cybersecurity but is also utilized by cybercriminals.

Artificial intelligence evokes strong emotions, which is why it is essential to create appropriate legal regulations. The European Union is already working on the AI Act, and in October 2021, NATO defense ministers adopted an artificial intelligence strategy for NATO.[12] The purpose of these regulations is to define the framework for the use and design of AI, which is intended to help strengthen defense against cyberattacks.

4. The use of artificial intelligence to enhance digital security

Artificial intelligence (AI) is becoming an increasingly important element in strengthening cybersecurity, offering innovative solutions that significantly improve the efficiency and effectiveness of defensive actions. AI contributes to enhancing security in several key ways:[13]

1. Detection and Prevention of Attacks

AI-based systems have the ability to analyze vast amounts of data in real time, enabling the identification of suspicious behavior patterns that may indi-

[10] M. Chiesa, & L. Lodi, *AI in Cybersecurity: Practical Applications and Emerging Threats*, Wiley 2020.

[11] P. Nowak, & J. Łukasik, *Zastosowanie sztucznej inteligencji w wykrywaniu zagrożeń w sieci*, Wyd. WNT 2021.

[12] M. Chiesa, & L. Lodi, *AI in Cybersecurity: Practical Applications and Emerging Threats*, Wiley 2020.

[13] Y. Zhang, & X. Li, *Deep Learning and its Role in Cybersecurity*, Elsevier 2020.

cate potential attacks. With advanced machine learning, AI can adapt to changing attacker tactics and quickly respond to new threats. This flexibility minimizes the need for continuous manual error analysis, which, in turn, shortens the response time to incidents.

2. Automation of Defensive Processes

AI allows the automation of many tasks related to monitoring, analysis, and response to cyber incidents. Automating these processes enables security teams to focus on more complex problems, while routine tasks are efficiently handled by AI systems. This way, organizations can better manage their resources and enhance their ability to respond quickly to threats.

3. User Behavior Analysis (Behavioral Analytics)

AI can analyze the behavior of both internal and external users to identify potential risks and anomalies. Behavioral analysis enables rapid response to suspicious activities, such as unauthorized access attempts or data theft. As a result, it is possible to detect and neutralize threats early, before they can cause significant damage.

4. Threat Profiling and Attack Forecasting

AI's predictive capabilities allow for forecasting potential threats based on the analysis of historical data and trends. This enables organizations to take proactive measures to minimize the risk of attacks. Threat profiling also allows for better preparation for various attack scenarios, which increases the overall resilience of systems against cyber threats.

5. Integration with Security Systems

AI can be integrated with existing security systems, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). This allows AI to act as an additional layer of protection, analyzing network traffic and user activities in real time, enabling rapid detection and response to threats. Such integration enhances the effectiveness of existing defense mechanisms and provides more comprehensive protection.

6. Risk Management Optimization

AI supports risk management by analyzing and evaluating potential threats and recommending appropriate preventive actions. With advanced algorithms, AI can provide precise information about the most critical risks, enabling organizations to better plan and allocate resources. Optimizing risk management contributes to improving the overall effectiveness of security strategies.

7. Education and Training

AI can also be used for educating and training employees in cybersecurity. AI systems can simulate various attack scenarios, enabling realistic exercises and tests. This helps employees better prepare for real incidents, increasing the overall awareness and readiness of the organization to respond to threats.

8. Personalized Protection

Advanced AI systems allow for personalizing protection strategies based on the specific needs and threats faced by individual organizations. AI can adjust protective measures in real time, considering changing conditions and new information. Personalizing protection increases the effectiveness of defensive actions and minimizes the risk of overlooking critical threats.

9. Compliance Monitoring

AI helps organizations monitor compliance with legal regulations and industry standards. AI systems can automatically track and analyze changes in regulations, enabling quick adjustments to security policies and procedures. Compliance monitoring is essential for avoiding penalties and maintaining the company reputation at a high level.

10. Support in Post-Incident Investigations

AI can also support post-incident investigations by analyzing collected data and identifying the sources and causes of attacks. Advanced algorithms can process large volumes of information faster than humans, accelerating the process of identifying perpetrators and addressing the aftermath of an attack. AI support in investigations allows for more effective data recovery and minimizes losses after incidents.

5. The role of artificial intelligence in building a secure digital world

Leading players in the cybersecurity market are increasingly implementing artificial intelligence (AI)-based solutions, which serve not only to mitigate the effects of cyberattacks but also to prevent them. Many companies offer advanced technologies integrating autonomous protection systems that utilize, among other things, deep learning models and neural networks.[14] These solutions enable not only the standard collection and analysis of events across various parts of the IT infrastructure but also the suggestion of preventive actions that can be taken even before a threat occurs. As a result, AI is becoming an essential tool in effectively protecting against cyber threats.

In summary, artificial intelligence (AI) can be used for:[15]

- Detecting suspicious activities: AI has the ability to monitor network traffic in real-time, detecting logins from unknown IP addresses, unusual visits

[14] M. Aldosari, *AI-driven Security Systems: Safeguarding Networks in the Age of Artificial Intelligence*, Taylor & Francis 2020.

[15] M. Sienkiewicz, *Sztuczna inteligencja w cyberbezpieczeństwie: nowoczesne rozwiązania ochrony sieci*, Wyd. Helion 2019.

to websites, or attempts to access sensitive data by unauthorized users. This allows for quick identification of threats and malicious software.

- Analyzing cyber threats: AI analyzes vast amounts of data, detecting patterns and anomalies. AI-based applications monitor Network traffic, generate detailed analyses, and create reports, enabling effective prevention of the spread of malicious software and dangerous files.
- Creating secure software: AI supports developers by providing real-time feedback on code, which improves the quality and security of applications. This allows for the effective identification and elimination of security vulnerabilities during the software development stage.

AI-based solutions[16] significantly enhance the effectiveness of protective actions, enabling organizations to respond more quickly and effectively to cyber threats.

Summary

Artificial intelligence is transforming the field of cybersecurity by introducing modern and effective technologies that strengthen an organization's ability to defend against increasingly sophisticated threats. The use of AI in detecting and preventing attacks, automating defensive actions, analyzing user behavior, and forecasting potential threats allows for the creation of more resilient and secure digital systems. The integration of artificial intelligence with existing security solutions, streamlining risk management, personalizing protection, and supporting investigative processes are just a few of the advantages AI brings to the field of cybersecurity. With these technologies, organizations can more effectively protect their assets, respond faster to threats, and more efficiently minimize the risk of cyberattacks.

Cybersecurity has become one of the key priorities for organizations worldwide. In the face of an increasing number of cyberattacks and ever-more specialized threats, companies are increasingly turning to artificial intelligence and machine learning to strengthen their protection systems. AI technologies are the future of securing the digital world, and it is up to us whether we will use them to safeguard our businesses or become their victims. Artificial intelligence is revolutionizing the cybersecurity sector, offering powerful tools to combat cyber threats. Despite some challenges, its ability to quickly and accurately detect threats and respond instantly makes AI an invaluable component in the security strategies of any organization.

[16] P. Nguyen, & K. Lee, *Machine Learning for Cybersecurity: A Practical Guide*, Academic Press 2022.

As AI technology develops, its importance in preventing and combating cyber threats will continue to grow. In summary, the article presents artificial intelligence as a key element of future network defense strategies that can significantly improve the ability to detect and respond to cyber threats. Success in this area, however, requires continuous investment in technology development and the training of specialists.

Bibliography

Aldosari M., *AI-driven Security Systems: Safeguarding Networks in the Age of Artificial Intelligence*, Taylor & Francis 2020.

Bieliński W., & Kowalski J., *Sztuczna inteligencja w bezpieczeństwie komputerowym: wyzwania i możliwości*, WN PWN 2020.

Chiesa M., & Lodi L., *AI in Cybersecurity: Practical Applications and Emerging Threats*, Wiley 2020.

ENISA, *Artificial Intelligence Cybersecurity Challenges: Threat Landscape for Artificial Intelligence*. European Union Agency for Cybersecurity 2020. Retrieved from https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

Hossain M.S., & Muhammad G., *Artificial Intelligence for Cybersecurity: Foundations, Techniques, and Applications*, CRC Press 2021.

Kowalski M., *Automatyzacja procesów ochrony w cyberbezpieczeństwie przy wykorzystaniu AI*, Wyd. Wydziału Informatyki Politechniki Warszawskiej 2023.

Nguyen P., & Lee K., *Machine Learning for Cybersecurity: A Practical Guide*, Academic Press 2022.

Nowak P., & Łukasik J., *Zastosowanie sztucznej inteligencji w wykrywaniu zagrożeń w sieci*, Wyd. WNT 2021.

Raj M., & Sharma A., *Artificial Intelligence and Cybersecurity: Enhancing Network Defense*, Springer 2021.

Sienkiewicz M., *Sztuczna inteligencja w cyberbezpieczeństwie: nowoczesne rozwiązania ochrony sieci*, Wyd. Helion 2019.

Williams J., & Taylor D., *The Future of Cybersecurity: AI and Machine Learning in Network Defense*, Springer 2021.

Zhang Y., & Li X., *Deep Learning and its Role in Cybersecurity*, Elsevier 2020.

Zieliński K., *Bezpieczeństwo cyfrowe w erze sztucznej inteligencji*, Wyd. Akademickie Dialog 2022.