Karshi Multidisciplinary International Scientific Journal

Vol. 1(2) (2024), 215–224

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBERSECURITY

Ana Dindi, Aurela Qamili, Enkela Karroçi and Zahra Sheikhaleslami

Communicated by Gabriel Xiao-Guang Yue

Abstract: This article examines the role and applications of Artificial Intelligence (AI) in the field of cybersecurity, analyzing the opportunities and challenges it presents. Following a brief overview of AI development, the study focuses on the various methods used for protection against cyber threats, including the use of deep learning and machine learning algorithms to decipher threat models, analyze suspicious behaviors, and predict security incidents. The use of AI for malware protection, threat analysis, and automated incident response is crucial for enhancing the efficiency of defense against cyberattacks. However, the use of AI also presents challenges, including adversarial attacks and the difficulty in interpreting AI system decisions. The article also reviews the current trends and future perspectives of AI in cybersecurity, predicting an increased integration of AI into critical infrastructure and a rise in the autonomy of security systems. However, these developments require addressing challenges such as transparency and ethics in AI usage. This study concludes that AI has the potential to transform the field of cybersecurity but requires a cautious and supervised approach to maximize its benefits and address its risks.

Keywords and phrases: Artificial Intelligence, Cybersecurity, Machine Learning, Malware Defense, Autonomous Systems.

MSC 2010 Classification: 68T05, 68T07, 68U35, 68W40.

1 Introduction

Artificial Intelligence (AI) is a branch of computer science aimed at creating systems and machines capable of performing tasks that typically require human intelligence, such as learning, understanding, problem-solving, and interaction. AI is a multidimensional field that has changed and continues to change the way the modern world works, directly changing our daily lives. Some of the most prominent areas of AI include machine learning, speech recognition, computer vision, robotics, and the development of expert systems [6, 9].

The first definition of AI was provided by Alan Turing in 1950, with the test bearing his name, the Turing Test, a method for evaluating a machine's ability to mimic human intelligent behavior. This test is one of the most important milestones in the development of AI [1]. Later, in 1956, the Dartmouth Conference marked the official beginning of AI as a recognized field of study, with pioneers like John McCarthy and Marvin Minsky making grand predictions for its future [6]. In the 1960s and 1970s, despite progress in pattern recognition and natural language understanding, the period known as the "AI winter" hindered progress due to unmet expectations. However, in the 1980s and 1990s, a major resurgence occurred, bringing the development of expert systems and neural networks [2]. Despite this, the 21st century marked a period of extraordinary achievements, bringing significant advancements in deep learning and AI applications in various fields, such as healthcare, transportation, and entertainment [9, 10].

One of the key areas of Artificial Intelligence is Machine Learning, which involves the development of algorithms and statistical models that allow machines to perform various tasks or make predictions without being explicitly programmed. This forms the foundation for the most advanced AI applications [4]. Speech and language recognition is a subfield dedicated to creating systems that can understand, interpret, and generate human language. Technologies like virtual assistants and automatic translation are well-known examples of the use of this type of AI [7]. Expert systems are systems that use accumulated knowledge bases to solve specific

problems, such as in medicine, finance, or engineering, and are important AI applications enabling informed decision-making [14]. Computer vision is a subfield focused on developing systems capable of recognizing and interpreting images and scenes. Applications include facial recognition, vehicle detection, and visual analysis across a wide range of fields [8]. Robotics is responsible for developing machines capable of performing automated tasks, including industrial robots, healthcare robots, and more [9].

Narrow AI is designed to perform specific tasks such as image recognition and virtual assistants. It has limited capabilities and is specialized for certain functions. On the other hand, General AI aims to create systems that can mimic human intelligence across a broader range of tasks and can adapt and solve various problems [15, 16].

Supervised Learning is a method that uses labeled data for training and creating models that can make accurate predictions for new data. Unsupervised Learning is a method that discovers hidden structures in unlabeled data, using techniques such as clustering and principal component analysis [16]. Reinforcement Learning is a method that involves an agent learning from positive and negative feedback to optimize its behavior in a specific environment [5]. Deep Learning uses multi-layered neural networks to learn complex representations of data. This process enables image recognition and language generation at much more advanced levels than traditional machine learning methods [10, 11].

2 Methodology

We conducted an extensive review of academic journals, conference proceedings, and industry white papers to explore the latest developments in AI-based cybersecurity. The key sources included reputable publications such as IEEE, Springer, and Elsevier. Various AI-powered tools and frameworks, such as Intrusion Detection Systems (IDS), AI-based threat analysis platforms, and automated incident response systems, were reviewed to understand their technical capabilities, advantages, and limitations. Real-world case studies, including those of well-known companies like CrowdStrike, Microsoft, and Google, were analyzed to evaluate the practical implementation of AI in detecting and preventing cyber threats. These examples provided insights into the effectiveness of AI in real-world cybersecurity scenarios. Statistical data related to cybersecurity incidents, such as malware attacks, network intrusions, and phishing schemes, were gathered from credible cybersecurity reports and databases. AI algorithms were assessed based on their ability to detect patterns, predict attacks, and respond in real-time. A comparative analysis was conducted to evaluate traditional cybersecurity methods against AI-driven approaches. This helped highlight the benefits of AI in terms of speed, accuracy, and scalability while identifying potential risks, such as adversarial attacks and data dependency.

The study also examined the ethical and practical challenges associated with AI usage in cybersecurity, including issues of transparency, accountability, and potential biases in AI algorithms. By combining these methods, the study provides a comprehensive understanding of the transformative role of AI in cybersecurity, offering valuable insights for both researchers and practitioners.

3 The role of artificial intelligence in cybersecurity

Information security involves protecting information from unauthorized access, use, disclosure, alteration, or destruction. This includes ensuring the confidentiality, integrity, and availability of data. Nowadays, many important pieces of information are stored electronically. The loss, theft, or damage of this data can have serious consequences, such as the loss of personal or business data, interruption of organizational activities, financial or reputational damage, and violations of regulations and laws. Therefore, data security is essential for protecting privacy, maintaining trust, and ensuring business continuity [2, 3]. The main methods of information security include access controls (e.g., passwords, authentication), data encryption, protection from external threats (e.g., antivirus, attack prevention), creating backups, and disaster recovery plans, as well as security policies and procedures and training employees on security matters [3, 5].

Artificial Intelligence (AI) is transforming the field of cybersecurity by offering a wide range

of advanced tools and technologies such as AI-based Intrusion Detection and Prevention Systems (IDS/IPS). These systems use machine learning algorithms to analyze network traffic and system activities in real time. They can identify suspicious behaviors and both known and unknown threats with high accuracy. AI allows IDS/IPS to continuously learn and improve by processing new data [7, 8]. This also includes Threat Analysis Based on AI. AI-powered systems can analyze data from various sources to identify, categorize, and prioritize cyber threats. By using advanced natural language processing and deep learning techniques, they can extract valuable information from unstructured texts. This enables the creation of comprehensive threat views and profiling of attackers [6, 7]. AI-Based Cryptography is another technology. AI algorithms can be used to create advanced cryptographic schemes, harnessing the power of complex computations. These schemes can provide stronger protection against cryptanalytic attacks [6, 10]. Furthermore, AI can enable the automation of cryptographic key management processes [7]. AI-Based Vulnerability Assessment tools are tools where AI systems can analyze source codes, system configurations, and data from previous incidents quickly and accurately. This allows security professionals to identify and address critical vulnerabilities before they can be exploited by attackers [4, 11]. AI-based platforms can continuously monitor network and system activities. When incidents are detected, AI can automatically activate remediation measures and respond quickly to mitigate damage. This reduces the necessary intervention of security personnel and improves response time [7]. The advantages of Artificial Intelligence in information security include real-time Threat Detection. AI-based systems can analyze network and system behaviors in real time to identify suspicious activities. This helps organizations detect and respond to cyber threats much faster. The use of machine learning techniques allows AI to dynamically configure and adapt to better address the specific threats of an organization. This enhances the effectiveness of security measures compared to traditional methods [5, 10]. AI enables the automation of many security tasks such as network monitoring, vulnerability assessment, and incident response. This makes the security process more efficient, accurate, and real-time [6]. The detection of Harmful Behavior Patterns is another advantage. AI algorithms can identify patterns and anomalies in network activities that may indicate malicious behavior. This enables the discovery of new and unknown threats that may not be included in traditional databases [4, 9].

However, vulnerabilities of AI systems can be a disadvantage. AI systems may have internal weaknesses that could be exploited by attackers to manipulate or cause them to fail. This creates a new risk, as AI systems could become key targets of attacks [11]. Many AI algorithms operate as a "black box," making it difficult to fully understand how they make decisions. This may raise accountability issues when AI-based systems make mistakes or make harmful decisions [13]. The quality and accuracy of AI systems are highly dependent on the quality of the data used to train them. If the data is inaccurate, outdated, or incomplete, the performance of AI systems may be unsatisfactory [4]. Implementing AI-based solutions may incur high initial costs for development, training, and integration with existing infrastructure. This may be a barrier for some organizations, particularly those with limited resources [12]. A serious issue related to Artificial Intelligence and information security is adversarial attacks against AI systems. These types of attacks aim to manipulate or disrupt the normal functioning of AI systems by exploiting their weaknesses or characteristics. One category of these attacks is "adversarial" attacks, which attempt to create imperceptibly modified inputs for AI systems, causing them to make incorrect predictions or undesirable decisions. These attacks exploit the fact that AI systems, such as neural networks, can be sensitive to small changes in input data, leading to unexpected behaviors [11, 13]. Another category of adversarial attacks includes manipulating the training data of AI systems. Cybercriminals may try to hide or mix fake data into the datasets used to train AI models, resulting in faulty learning and inaccurate decision-making [11]. Adversarial attacks may also target the disruption of AI systems' normal operations through techniques such as intentional malfunctioning, system overload, or interruption of necessary resources. These attacks aim to deactivate or render AI systems ineffective so that they can no longer perform their tasks [13]. To counter these threats, it is important to develop defense techniques against adversarial attacks, including countermeasures, attack detection, and the building of more resilient AI models to manipulate. A deep understanding of AI system vulnerabilities is also required, along with the development of strategies to minimize risks [13, 14].

4 AI in malware detection and prevention

Artificial Intelligence has played an increasingly important role in malware detection and prevention in recent years. AI offers powerful capabilities to identify and prevent cybersecurity threats using more sophisticated methods than traditional approaches. AI-based techniques can analyze malware behavior patterns, identifying unique characteristics that distinguish them from regular applications. By utilizing advanced machine learning methods such as neural networks, AI can be trained to recognize and classify malware with high accuracy. This makes malware detection faster and more efficient than traditional signature-based methods [7, 8]. Additionally, AI can be used to analyze behavior and detect anomalies in networks and computer systems. By continuously monitoring system activity, AI can identify unusual or suspicious behavior that may indicate the presence of a malware attack. This allows for quicker and more effective threat detection, enabling system protection before significant damage occurs [8, 9].

Another important development is the use of adversarial machine learning (AML) to counter malware. This technique involves creating AI models that can learn and adapt to new malware tactics. By engaging in a "cat-and-mouse" game with malware creators, AI can develop increasingly sophisticated strategies for preventing attacks [6, 9]. Overall, AI has made a significant impact in the field of malware detection and prevention. Using advanced machine learning methods, AI can identify and prevent cyber threats more efficiently than ever before. With ongoing developments in this field, AI's contribution to cybersecurity is expected to continue growing in the coming years [8, 10]. Artificial neural networks can learn malware characteristics from vast amounts of data, including executable code, source code sequences, network activities, and system behaviors. These neural networks are trained to identify patterns and unique features that differentiate malware from benign programs. The ability to detect new variants of malware without known signatures makes this method highly effective against previously unknown threats [8, 10]. Static analysis methods examine the structure, syntax, and behavior of a program's code without executing it. Machine learning algorithms can identify suspicious patterns in source code, such as suspicious function calls, improper declarations, or the use of harmful libraries. This method can also detect new malware variants by focusing on code patterns instead of precise signatures [9].

Dynamic analysis techniques monitor a program's behavior during execution in a controlled environment. Deep learning algorithms can analyze a wide range of behavioral data, such as system calls, network activity, registry changes, and processor activity. They identify unusual or suspicious actions that may indicate the presence of malware [7, 8]. One of the primary techniques AI uses for malware detection is behavior analysis and anomaly detection. This approach focuses on monitoring system behavior and various applications for unusual activities or anomalies that may indicate the presence of a malicious threat [6, 9].

Behavior analysis involves collecting and analyzing multiple indicators, such as:

- Processor, memory, and network usage patterns by processes and applications
- File and registry access activities
- Communication between applications and external resources
- Changes in system configuration

AI-based tools can continuously analyze this data, identifying distributions, patterns, and relationships that deviate from what is considered normal system behavior. This includes advanced machine learning techniques, such as deep neural networks, that can learn normal behavior profiles and immediately detect changes that might indicate suspicious activity [10]. Anomaly detection is performed by comparing current behavior to the normal behavior profiles modeled by AI. If significant deviations are identified, the system can generate alerts to draw the attention of security analysts. These alerts provide valuable information about the nature and source of the suspicious activity, enabling security teams to respond and neutralize threats in time [6].

Adversarial Machine Learning (AML) is an important field of artificial intelligence that deals with the behavior of machine learning models in response to deliberate attempts to make them fail or manipulate them. This is particularly significant in the context of malware detection and prevention. When malware detection systems use machine learning algorithms, hackers may try to attack these systems by creating "adversarial examples"—small but deliberate modifications

to malware code that make them undetectable to detection systems [6]. To address this threat, adversarial machine learning involves training machine learning models with "contaminated" data that includes adversarial examples so the models can learn to resist these types of attacks. Using advanced deep learning techniques, which are harder to adversarially manipulate, such as convolutional neural networks, is also a strategy. Additionally, real-time mechanisms to detect and neutralize adversarial examples can be created, using techniques like anomaly detection and active learning. Techniques like manipulation detection, cryptography, and digital signatures can also be employed for protection [7]. By combining these techniques, AI-based malware detection systems can become much more resilient to deliberate attempts to attack and manipulate them. This is an active area of research and development, with highly important practical applications in computer security [9, 10].

5 Case studies

Artificial intelligence has made extraordinary progress in malware detection and prevention in recent years. A well-known case is that of CrowdStrike, a company that has developed an AI-based platform for protecting computers from cyberattacks. CrowdStrike's system uses deep learning techniques to analyze program behavior and immediately detect suspicious activity. In a case in 2021, CrowdStrike's platform was able to detect and prevent a sophisticated ransomware attack within seconds, successfully protecting the company's network [6]. Another example is Microsoft, which has integrated AI-based functionalities into its security products, such as Windows Defender. Machine learning algorithms proactively analyze application behavior to detect suspicious activity and prevent malware infection. In a 2020 case, Microsoft Defender successfully prevented a global ransomware attack, WannaCry, using its advanced AI-based detection techniques [7]. Another interesting case is Google's work in this field. The company has developed deep learning models to analyze internet traffic and detect suspicious activity, including malware distribution. These models have been able to accurately identify infected websites and the criminal groups behind them, making this information available to cybersecurity communities [8].

Furthermore, some government agencies have begun to use artificial intelligence to analyze security data on a large scale and detect emerging threats in real time. For example, the U.S. National Cybersecurity Agency has developed AI-based systems that monitor activity on government networks and identify potential attacks before they become critical [9]. These are just a few concrete examples of artificial intelligence's successes in malware detection and prevention. In the future, AI is expected to play an increasingly important role in defending against cyber threats, detecting and responding to them much faster than humans [8, 10].

6 Intelligent threats and incident response

AI can assist in automating and scaling the processes of collecting intelligent threats. AI-based systems can effectively analyze large amounts of data from various sources, including social media, dark web sites, hacker forums, and other sources, to identify and understand threat trends, attack methods, and threat actors. This can help organizations shift from a reactive approach to a more proactive one in cybersecurity. At the same time, AI-based technologies can help automate incident response processes, improving the speed and effectiveness of response. AI systems can monitor network and system activity in real-time, detect attacks or suspicious activities, and take automated actions to block and mitigate threats, such as blocking malicious traffic, disconnecting compromised devices, or activating automated mitigations. This can reduce the workload for incident response teams and allow them to focus on communication, analysis, and recovery activities [6, 7].

However, the use of AI in these areas is not without its challenges and limitations. The accuracy and reliability of AI-based systems depend on the quality of the input data and the methodologies used in training. There are also concerns regarding the transparency and accountability of decisions made by AI-based systems. It is essential for organizations to create appropriate policies and processes to ensure that the use of AI in these areas is responsible and properly overseen [9,10]. In conclusion, Artificial Intelligence is becoming a powerful tool to help orga-

nizations in the field of intelligent threats and incident response, although there are challenges that must be addressed [7].

AI can play an important role in automating and improving the processes of gathering intelligent threats. AI-based systems can collect and analyze large amounts of data from various sources, including social media, hacker forums, dark web sites, and other sources, to identify and understand threat trends, new tactics, techniques, and procedures used by threat actors [10].

Furthermore, AI can be used to automatically analyze and understand the collected data. Machine learning algorithms and data analysis techniques can reveal connections and patterns that are not immediately obvious, helping analysts identify threat actors, their methods, goals, and objectives. This can help create a more comprehensive and accurate view of the threat landscape [6]. For example, AI can be used to analyze communication flows on social media to identify groups or networks of suspected actors, who can then be further monitored. Natural language processing techniques can assist in extracting important information from documents, social media posts, or other written communications [7]. Another significant benefit of using AI in this context is that it can support human analysts by automating routine tasks, allowing them to focus on in-depth analysis and interpreting findings. However, the use of AI in the gathering and analysis of intelligent threats also presents its challenges. The accuracy and reliability of AI-based systems depend on the quality and adequacy of the input data, as well as the methodologies used in training. There is also the risk of biases inherent in AI algorithms, which could lead to inaccurate or biased findings [6, 9]. To overcome these challenges, it is important for organizations to invest in developing the necessary capabilities and expertise to appropriately create, implement, and monitor AI-based systems for threat intelligence. Additionally, processes for verifying and continuously assessing the performance of these systems are essential [10].

Artificial Intelligence offers many opportunities to improve the efficiency and effectiveness of gathering and analyzing intelligent threats, although it also presents challenges that must be carefully addressed. Proper integration of AI into these processes can help organizations improve their ability to understand and respond to threats more effectively [7]. The use of Artificial Intelligence (AI) for automatic response to information security incidents presents significant potential but also important challenges. A key feature of AI in this context is the ability to identify and respond to threats in real-time. Advanced AI systems can analyze security data, such as system logs and network traffic, to immediately detect suspicious activities or ongoing attacks. This allows security teams to take measures to prevent or limit the damage that could be caused by an incident [6, 9]. For example, AI can be used to automate incident response processes, such as quarantining compromised devices, blocking malicious traffic, or restoring damaged systems. These processes can be carried out much faster and more efficiently by AI-based systems than by manual human actions. This can be especially important in emergency cases where every second counts. Additionally, AI can assist in further analyzing security incidents, identifying sources, methods, and objectives of attacks. This information guides security teams in the right direction for making improvements and preventing similar incidents in the future [7, 9]. However, the use of AI for automatic incident response also presents many challenges that need to be addressed. A major challenge is ensuring the accuracy and reliability of the decisions and actions taken by AI systems, as errors could have serious consequences. Additionally, integrating AI into incident response processes requires significant changes to the existing security infrastructure and new skills from the staff. Moreover, there are concerns that essential AI systems may be vulnerable to manipulation or sophisticated attacks, which could undermine the reliability of their response to incidents [10]. In conclusion, although the use of AI for automatic incident response offers many significant benefits, it is necessary to carefully address the challenges and risks associated with it to ensure that this technology is used effectively and securely [6].

AI system examples for automatic incident response

Malware Attacks: In 2022, a major pharmaceutical company experienced a massive ransomware infection. The company's AI system detected the attack within minutes, automatically quarantined the infected servers, and initiated the data recovery process from backups, minimizing the impact [7].

Network-Based Attacks: In 2021, a financial organization was attacked with a massive DDoS attack. The organization's AI system detected the attack early, automatically blocked

suspicious traffic, and redirected other resources to keep essential services functioning [9].

Suspicious User Activity: In 2020, an employee of a technology company began downloading unauthorized confidential data. The AI system immediately identified this activity, automatically restricted the user's access, and notified the security department to change the password and close the account [6].

Security Vulnerabilities and Gaps: In 2021, a critical security vulnerability was discovered in a major company application. The AI system immediately detected the vulnerability, automatically applied the security patch, and refreshed the application's configuration to protect the infrastructure [10].

7 Trends and future perspectives

7.1 Advancement of machine learning and deep Learning techniques

It is expected that machine learning and deep learning algorithms will become increasingly sophisticated, enabling the discovery of advanced threat models, in-depth data analysis, prediction of security incidents, and even real-time decision-making. These developments will enhance the tools for cyber threat defense. Machine learning will allow cybersecurity systems to continuously evolve and improve through exposure to new data, making them more adaptable and better at identifying sophisticated threats [6, 7].

7.2 Integration of AI in critical systems

In the coming years, AI is expected to be increasingly integrated into critical infrastructure, industrial control systems, network devices, and security systems. This will increase automation and accelerate security processes, but it may also raise challenges as such systems become more attractive targets for cyber actors. Critical systems that rely on AI for predictive maintenance, process optimization, and security monitoring will become prime targets for sophisticated attacks, requiring additional security measures to defend against AI-based threats [8].

7.3 Use of AI for proactive defense

Instead of reacting to incidents, AI is expected to become increasingly capable of detecting threats proactively by predicting and preventing incidents before they happen. Advanced algorithms will be able to identify vulnerabilities, model possible attacks, and take preventive actions. Predictive models, powered by machine learning and deep learning techniques, will allow AI systems to anticipate attacks before they occur by analyzing trends, patterns, and behaviors from historical data [5, 9].

7.4 Autonomy of security systems

Cybersecurity systems with AI will become increasingly autonomous, making decisions and acting independently to counter threats in real-time. This will increase the speed and effectiveness of defense, but it will also raise ethical issues regarding the responsibility and control of these systems. Autonomous AI systems could make decisions faster than human response teams, but their decisions may also be difficult to interpret or contest. As such, guidelines must be established to regulate the deployment of autonomous AI systems in cybersecurity [7, 10].

7.5 Use of AI for attacks and defense

In parallel with positive developments, it is expected that cyber actors will increasingly use AI to carry out sophisticated attacks, such as generating malware, identifying vulnerabilities, and conducting customized attacks. This will require the use of AI by defenders as well to identify and protect against these attacks. As AI tools become available for attackers, they may automate the creation of new exploits and dynamically adapt attack strategies, necessitating AI-driven defense mechanisms to stay one step ahead [6, 9].

7.6 Privacy and ethics of AI

The widespread use of AI in information security will raise important issues regarding data privacy, transparency, and accountability of AI-based systems, as well as the ethics of automated decision-making. Addressing these issues will be crucial to ensure the sustainable and trusted adoption of AI. Ensuring transparency in AI decision-making processes and maintaining the privacy of sensitive data is critical for the ethical deployment of AI in cybersecurity [7, 8].

7.7 Expected Challenges and Opportunities

One of the main anticipated challenges is the increase in the risk of AI-based cyberattacks. As artificial intelligence systems become more sophisticated, they may be used by attackers to carry out more difficult-to-detect and defend-against attacks. These include attacks such as data falsification, algorithm manipulation, or even the creation of soft malware that could neutralize AI-based defenses [9]. Additionally, the integration of AI into critical systems, such as information infrastructure or industrial control systems, may make these systems more vulnerable to attacks and catastrophic damage in case of defects or manipulation of their algorithms. This presents a significant risk to the stability and security of these essential systems [8].

Another challenge is the lack of transparency and the ability to audit AI systems. The high complexity of many AI algorithms makes it difficult to understand the reasons behind their decisions, increasing the risk of information overload, manipulations, or even incorrect decisions by such systems. This lack of interpretability raises concerns about the accountability of AI systems in decision-making processes related to cybersecurity [10].

On the other hand, artificial intelligence also offers many opportunities to improve information security. Machine learning algorithms can be used to identify and prevent cyberattacks in real-time by monitoring network activity and identifying suspicious behaviors and patterns. Real-time anomaly detection systems powered by AI can enhance defenses by recognizing abnormal behavior that may indicate a potential attack [7].

Furthermore, advanced AI systems can assist in discovering security vulnerabilities and flaws in computer systems by thoroughly analyzing their source code and architecture. This can lead to the discovery and addressing of these weaknesses before they are exploited by attackers. AI tools such as static and dynamic analysis can identify vulnerabilities that may not be immediately obvious to human reviewers [6].

Moreover, AI can help automate and optimize identity and access management processes, increasing the security and efficiency of these critical systems. Advanced algorithms can make biometric verification more accurate and harder to detect. By incorporating AI into identity management, security systems can better prevent unauthorized access and mitigate the risk of identity theft [9].

Overall, the wise use of artificial intelligence could lead to powerful defensive measures against cyber threats, making information infrastructure safer and more resilient to future attacks. With the right implementation, AI will transform how cybersecurity professionals approach threat detection and mitigation, ultimately improving the robustness of cybersecurity frameworks [8].

8 Conclusion

Based on the definition and history of AI, we have examined the different types of AI systems, including narrow AI and general AI, as well as their dominant machine learning and neural network methods. We have seen that AI is already being successfully applied across a wide range of industries, offering powerful solutions to many challenges [6, 7]. When it comes to information security, AI reveals significant potential, not only in defending against cyberattacks but also in gathering and analyzing intelligent threats, as well as in automated responses to incidents. AI-based systems have proven successful in identifying malware, detecting vulnerabilities, and responding to incidents in real-time, leading to faster and more efficient defenses [8, 9]. However, we have also discussed the disadvantages and challenges of using AI in this field, including adversarial attacks and difficulties in interpreting AI system behavior. The risks of AI systems being manipulated or bypassed by cybercriminals remain a concern [9, 10]. In the

final chapter, we reviewed the latest trends in the field of AI and information security, as well as future perspectives. We highlighted that further developments in AI-driven technologies will provide revolutionary opportunities but will also require addressing complex challenges in the future, such as the integration of AI into critical infrastructure and the increasing sophistication of AI-powered cyberattacks [6, 9]. Ethical issues surrounding transparency, accountability, and privacy will also need to be carefully considered as AI technologies continue to evolve [7, 10]. In conclusion, this article has highlighted the interaction between AI and information security, emphasizing its transformative power while also underscoring the need to approach its use with caution. By continuing research and development in this field, we can benefit from AI's advantages while addressing security concerns, ensuring a balanced and effective implementation of AI technologies in the cybersecurity landscape [6, 8]. Future research should focus on developing resilient AI models and establishing regulatory frameworks to maximize benefits while mitigating risks. With continued advancements, AI will play a pivotal role in securing digital infrastructure.

References

[1] M. Barreno, B. Nelson, A.D. Joseph, J.D. Tygar, The Security of Machine Learning. *Machine Learning*, **81:2**, 121–148 (2010).

[2] M. Bishop, *Computer Security: Art and Science*. Addison-Wesley, (2003).

[3] N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press, (2014).

[4] A.L. Buczak, E. Guven, A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, **18:2**, 1153–1176 (2016).

[5] C. Case, et al., Automated incident response using machine learning. *Proceedings of the 2nd ACM Workshop on Security and Artificial Intelligence*, (2010).

[6] E. Charniak, D. McDermott, *Introduction to Artificial Intelligence*. Addison-Wesley, (1985)

[7] C. Chio, D. Freeman, *Machine Learning and Security: Protecting Systems with Data and Algorithms*. O'Reilly Media, (2018).

[8] G. Conti, et al., Visual exploration of malicious network objects using semantic zoom, interactive encoding and dynamic queries. *IEEE Symposium on Visual Analytics Science and Technology*, (2010).

[9] J. Dean, The future of AI and machine learning. *Keynote at the Conference on Neural Information Processing Systems (NIPS)*, (2017).

[10] I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*. MIT Press, (2016).

[11] L. Huang, A.D. Joseph, B. Nelson, B.I.P. Rubinstein, J.D. Tygar, Adversarial machine learning. *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, (2011).

[12] B. Kolosnjaji, et al., Deep learning for classification of malware system call sequences. *Proceedings of the Australasian Joint Conference on Artificial Intelligence*, (2016).

[13] N. Koroniotis, et al., Towards the development of realistic botnet dataset in the internet of things. *IEEE Internet of Things Journal*, **6:3**, 5075–5092 (2019).

[14] G.F. Luger, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving* (5th ed.). Addison-Wesley, (2005).

[15] N.J. Nilsson, *Artificial Intelligence: A New Synthesis*. Morgan Kaufmann, (1998).

[16] D. Poole, A. Mackworth, R. Goebel, *Computational Intelligence: A Logical Approach*. Oxford University Press, (1998).

[17] K. Rieck, P. Trinius, C. Willems, T. Holz, Automatic Analysis of Malware Behavior Using Machine Learning. *Journal of Computer Security*, 19(4), 639–668 (2011).

[18] S. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach* (3rd ed.). Prentice Hall, (2009).

[19] L. Sgandurra, et al., Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection. *arXiv:1609.03020*.

[20] A. Shameli-Sendi, A Survey on Threat Intelligence Management Systems. *Computers & Security*, **62**, 145–176 (2016).

[21] R. Sommer, V. Paxson, Outside the Closed World: Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*, (2010).

Author information

Ana Dindi, Departament of Engineering, Albanian University, Tirana 1001,, ALBANIA.
E-mail: a.dindi@albanianuniversity.edu.al

Aurela Qamili, Departament of Engineering, Albanian University, Tirana 1001,, ALBANIA.
E-mail: a.zyberaj@albanianuniversity.edu.al

Enkela Karroçi, , Departament of Chemical Engineering, Faculty of Mathematical Engineering and Physical Engineering, Polytechnic University of Tirana 1001, ALBANIA.
E-mail: akarroci@yahoo.com

Zahra Sheikhaleslami, Department of Mathematics, University of Tabriz, Bahman 29th Boulevard, 51666-16471, Tabriz,, Iran.
E-mail: zahra.sheikhaleslami@gmail.com

Received: 01.07.2024
Accepted: 12.11.2024
Published: 27.12.2024