# Artificial Intelligence with Respect to Cyber Security

Syed Adnan Jawaid
Department of Computer Science, Washington University of Science and Technology, Vienna, Virginia. VA 22182 USA.

* Corresponding author. Email: adnan.jawaid@hotmail.com (S.A.J.)
Manuscript submitted April 26, 2023; accepted May 15, 2023; published August 14, 2023.
DOI: 10.18178/JAAI.2023.1.2.96-102

**Abstract:** Artificial Intelligence has transformed the cyber security industry by enabling organizations to systematize and enlarge outdated safety procedures. AI can provide more effective threat detection and response capabilities, enhance vulnerability management, and improve compliance and governance. AI technologies such as machine learning, natural language processing, behavioral analytics, and deep learning can enhance cyber security defenses and protect against a wide range of cyber threats, including malware, phishing attacks, and insider threats. Theoretical underpinnings of AI in cyber security, such as machine learning, natural language processing, behavioral analytics, and deep learning, are discussed. The advantages of using AI in cyber security are discussed including speed and accuracy, continuous learning and adaptation, and efficiency and scalability. It's important to note that AI is not a silver bullet for cyber security and should be used in conjunction with other security measures to provide a comprehensive defense strategy. AI has transformed the way cyber security operates in today's digital age. By analyzing vast amounts of data quickly and accurately it has become a valuable tool for organizations looking to protect their assets from cyber threats.

**Keywords:** Artificial intelligence with respect to cyber security, artificial intelligence and cyber security, AI and cybersecurity, importance of AI with respect to cyber security

## 1. Introduction

The study of creating robots which are performing activities that traditionally require human intelligence including speech recognition, decision-making, and learning, is known as artificial intelligence (AI), and it is a subject of computer science that is expanding quickly. AI has important ramifications for cyber security, as it may be used to monitor vulnerabilities, detect and respond to threats, and maintain regulatory compliance [1]. In the digital age, where businesses and individuals are more susceptible to cyberattacks and data breaches due to increased use of technology and data, cyber security is a crucial concern. In this regard, AI has shown promise as a way to address the issues related to cyber security.

It subfield of computer science which aims to build robots which can perform activities that would typically need human intelligence which include speech recognition, decision-making, and learning. Cybersecurity has emerged as a critical issue as individuals and businesses are more vulnerable to cyberattacks and data breaches in the digital age. Integrating AI with cyber security is a practical strategy for dealing with difficulties related to cyber security. This essay will look at how AI is used in cyber security, as well as its advantages, disadvantages, and future prospects.

In order to completely comprehend the significance of cyber security in the digital era, it is essential to underline that the world is becoming more interconnected through the internet and other digital

technologies. With the rising use of social media platforms, cloud computing, and Internet of Things (IoT) devices, data and information flows through the internet have multiplied tremendously. This has sped up communication, improved the efficiency of transactions, and made it simpler for consumers to access services. However, it has also rendered people and businesses more vulnerable to new types of cyberthreats. These dangers include straightforward phishing attacks as well as sophisticated APTs that have the potential to penetrate huge networks and steal critical data.

## 2. Theoretical Underpinning

Some of the relevant theories that underpin the use of AI in cyber security include:

### 2.1. Machine Learning

Machine learning is a subset of AI that enables systems to automatically learn and improve from experience without being explicitly programmed [2]. Machine learning algorithms can be trained to detect patterns in data, which can be used to identify potential threats and vulnerabilities in cyber security.

### 2.2. Natural Language Processing

Another crucial component of AI that is utilized in cyber security is natural language processing (NLP). In order to look for potential cyber threats in unstructured data sources like social media, blogs, and forums, NLP enables machines to comprehend and analyze human language.

### 2.3. Behavioral Analytics

It is a method that makes use of AI to examine user behavior patterns and find anomalies that could be signs of a potential cyber threat. AI can identify potential security breaches and take appropriate action by observing user behavior on a network.

### 2.4. Deep Learning

Neural networks are used in deep learning, a subset of machine learning, to analyze and learn from data. Deep learning can be used to find patterns in data related to cyber security that may be hard to find using conventional security measures.

Organizations can strengthen their cyber security defenses and guard against a variety of cyberthreats, such as malware, phishing attacks, and insider threats, by utilizing these and other AI technologies. To provide a thorough defense strategy, AI should be used in conjunction with other security measures since it is not a silver bullet for cyber security.

Threat intelligence analysis examines unstructured data sources, such as social media, using natural language processing (NLP) to identify potential risks. Additionally, cyber threat hunting driven by AI can be used to find and track advanced persistent threats (APTs) that may be hiding in a network and predictive analytics can be used to identify possible dangers before they happen.

Automating penetration testing, security controls and rules, vulnerability scanning and prioritization, and patch management are all part of vulnerability management. AI-powered vulnerability scanning solutions, for instance, can assist organizations in identifying and prioritizing problems that need to be fixed right once. AI can also be used to automate penetration testing, in which the system attempts to attack flaws to gauge how well current security measures work. AI can also be used to handle patching procedures, monitor regulatory compliance, and establish and enforce security standards.

AI is used in compliance and governance to monitor adherence to rules and policies, identify risks, and enforce adherence to them. AI can be used, for instance, to automate compliance reporting and monitoring, ensuring that businesses abide by laws like the Health Insurance Portability and Accountability Act (HIPAA)

and the General Data Protection Regulation (GDPR). By analyzing vast volumes of data, detecting potential risks and vulnerabilities, and suggesting suitable mitigation strategies, AI can also be used to assess hazards. By automatically identifying and preventing policy violations, AI can also be used to enforce policy compliance [3].

## 3. AI's Role in Cyber Security Applications

In the digital age, cyber security is more important than ever. The increasingly complex cyber threats can no longer be protected against with traditional security techniques. Businesses are using artificial intelligence (AI) to enhance their cyber security strategies as a result. AI has numerous applications in the cyber security industry.

### 3.1. Threat Detection and Response

Threat detection and retaliation are two of the most important uses of AI in cyber security. In order to analyses enormous amounts of data and find patterns and anomalies that could point to the presence of a cyber threat, machine learning techniques and natural language processing are used. This can be achieved by deploying intrusion detection systems, which use AI-powered algorithms to monitor network traffic for trends and anomalies that may indicate a security compromise. Additionally, advanced persistent threats (APTs) that can be hidden in a network can be found and tracked using cyber threat hunting powered by AI. Additionally, organizations can utilize predictive analytics to spot potential threats before they materialize, enabling proactive defense [4].

### 3.2. Vulnerability Management

Vulnerability management is another essential use of AI in cyber security. Solutions for vulnerability scanning enabled by AI help businesses find and priorities issues that need to be fixed. Vulnerability management includes automating penetration testing, security policies, and patch administration. Penetration testing, in which the system tries to exploit holes to evaluate how effectively current security measures function, can also be automated using AI.

### 3.3. Compliance and Governance

AI is used in compliance and governance to detect risks, monitor compliance with rules and policies, and enforce compliance. AI can, for example, be used to automate compliance reporting and monitoring, ensuring that companies follow by regulations like HIPAA and GDPR. AI can also be used to assess hazards by analyzing massive amounts of data, identifying potential dangers and weaknesses, and suggesting appropriate mitigation solutions. AI can be used to enforce policy compliance by automatically detecting and stopping policy infractions.

## 4. Advantages of AI in Cyber Security

In this digital era, artificial intelligence (AI) has fundamentally changed how cyber security functions. Artificial intelligence (AI) has developed into a useful tool for businesses wanting to safeguard their assets from cyber threats due to its capacity to analyze massive volumes of data rapidly and effectively. In this aspect, AI has a number of benefits over conventional cyber security techniques. In-depth discussion of benefits and an examination of how AI is bolstering cyber security measures are provided below

### 4.1. Speed and Accuracy

One of artificial intelligence's main advantages for cyber security is its ability to deliver real-time threat identification and response. By examining network traffic, AI algorithms can quickly identify any unusual behavior that might indicate a security flaw. Security personnel can therefore respond to the attack quickly

and lessen the damage it causes. As a result of their ability to analyze massive amounts of data and identify potential risks that human analysts might have missed, AI-powered security solutions are also more accurate and dependable than traditional ones.

### 4.2. Continuous Learning and Adaptation

Another significant advantage of cyber security is the potential for AI to improve and learn over time. By continuously monitoring security systems and reviewing security incidents, AI algorithms can discover patterns and gain insights that improve their efficacy and accuracy. By allowing security systems to react quickly to new threats and attack vectors, AI also makes it easier to stay one step ahead of hackers.

### 4.3. Efficiency and Scalability

It is faster and more precise as compared to human analysts at processing and analyzing massive amounts of information. This lessens the workload for security experts, allowing them to concentrate on jobs that are more challenging and sophisticated. In addition, AI-powered security solutions are highly scalable since they can analyze data from numerous sources and handle huge traffic volumes without noticeably degrading performance.

Thus, applying AI to cyber security has a number of benefits. It is a crucial tool for defending against cyber-attacks in the digital era due to its efficiency, scalability, continuous learning, and adaptive capabilities, as well as speed and accuracy in threat detection and response.

## 5. Challenges of AI in Cyber Security

In the area of cyber security, artificial intelligence (AI) has been hailed as having revolutionary potential. Artificial intelligence (AI) can assist in detecting dangers and taking action more quickly and efficiently than human analysts alone by utilizing cutting-edge algorithms and machine learning approaches. Nevertheless, despite all of its advantages, AI presents a number of problems for cyber security [5]. In this section, we'll talk about some of the biggest obstacles that businesses encounter when putting AI-powered security solutions in place.

### 5.1. Shortage of Cyber Security Professionals with AI Expertise

Significant issue organizations encounter when implementing AI-powered security solutions is a lack of AI-savvy cyber security specialists. Even while AI has the ability to automate many cyber security-related tasks, it still needs human supervision and input to work properly. To design, implement, and maintain security systems that are AI-powered, specialists in cyber security are required.

Only 25% of cyber security workers now have AI skills, according to a recent survey by the international consulting firm Capgemini. Organizations may find it challenging to handle AI-powered security measures due to the lack of AI knowledge, which may make them more susceptible to cyberattacks. Organizations may need to spend money on training programs and other activities to help their cyber security specialists gain the essential AI capabilities in order to handle this challenge.

### 5.2. Over-Reliance on AI Systems

Another problem with AI in cyber security is its overuse. Although AI has the potential to be a useful tool for identifying dangers and implementing defenses, it does have drawbacks [6]. AI-driven systems are nevertheless vulnerable to errors and assaults that take advantage of their flaws. Additionally, organizations may be more likely to miss possible risks and vulnerabilities that these systems are not intended to detect if they place an excessive amount of reliance on AI systems.

### 5.3. Ethical Concerns

In the context of cyber security, AI also raises a variety of ethical concerns. Some AI-powered systems, for instance, may produce unfair or unjust outcomes if they use biased or discriminatory data sources. Additionally, attacks against AI-powered systems may be conducted to take advantage of those shortcomings, which could have unanticipated results.

Organizations must make sure that their AI-powered technologies are developed and deployed in an ethical and responsible manner in order to allay these worries. This might require routinely reviewing AI-powered systems to make sure there is no bias or discrimination. Additionally, businesses must be liable for any unintended repercussions that may result from the use of AI-powered systems and be honest about it.

### 5.4. Cyber Security Skills Gap

The current skills gap in cyber security may get worse with the implementation of AI-powered protection solutions. Demand for cyber security experts with specialized knowledge and skills is projected to rise as organizations adopt new technology and approach to guard against assaults. However, there is currently a talent gap in the cyber security industry, making it challenging for businesses to find and keep the expertise they require.

Companies should fund training and development programs to assist current employees in acquiring the knowledge and skills required to address this challenge. Organizations may also need to think about different cyber security strategies, such as hiring outside contractors for parts of their work or employing cutting-edge technology that doesn't require a lot of specialized knowledge.

## 6. The Future of AI in Cyber Security

The application of AI in cyber security appears to be moving in the right direction, with a number of fresh innovations and trends on the horizon. One of the largest trends is the escalating use of AI-powered security solutions and systems. As the threat landscape continues to evolve and grow more complicated, there is a rising need for more sophisticated and intelligent security measures [7, 8]. AI-driven systems can provide faster, more accurate threat detection and response, as well as continuous learning and adaptation to new threats.

Integration of AI is another emerging trend with other security technologies, including blockchain and the Internet of Things (IoT). Blockchain technology can provide a secure and tamper-proof way of storing and sharing sensitive data, and AI can be used to analyze and interpret the data to identify potential threats or vulnerabilities. Similarly, to this, as IoT devices become more prevalent, AI can be used to secure and monitor them because they are frequently targets of cyberattacks.

Deep learning and natural language processing are two examples of cutting-edge AI algorithms and techniques that are helping to shape the future of AI in cyber security. These developments enable a more sophisticated analysis of unstructured data sources like social media and forums and can increase the precision and efficacy of threat detection and response.

The increasing use of AI-powered security tools and systems, integration with other security technologies, and improvements in AI algorithms and techniques all point to a bright future for AI in cyber security. The need for intelligent and adaptive security measures will only increase as the cyber security landscape changes, making AI a crucial part of upcoming cyber security strategies.

## 7. Suggestions and Recommendations

There is a list of suggestions and recommendations below:

### 7.1. Invest in AI Expertise

Organizations should place a higher priority on hiring and investing in training professionals who can create and implement AI-powered solutions given the dearth of cyber security professionals with this knowledge.

### 7.2. Strike a Balance between Human Oversight and Automation

Although AI can automate many cyber security-related tasks, it's crucial to strike a balance between automation and human supervision. Making strategic decisions and handling complex problems that call for critical thinking still require human intuition and expertise.

### 7.3. Continuously Monitor and Evaluate AI Systems

It's critical to continuously assess the performance of AI systems, spot any flaws or vulnerabilities, and modify security precautions as needed.

Collaborate and share information:

Given the constantly evolving nature of cyber threats, collaboration and information-sharing among organizations and cyber security professionals can help identify emerging threats and develop more effective solutions.

### 7.4. Stay Informed and up-to-date

For the purpose of staying ahead of evolving threats and ensuring compliance with pertinent laws and regulations, organizations should stay informed about the most recent advancements in AI and cyber security, including emerging technologies, best practices, and regulatory requirements [9, 10]

## 8. Conclusion

Artificial intelligence has had a significant impact on the field of cyber security. AI is an essential tool for organizations to defend against attacks, uncover weaknesses, and handle crises as a result of the complexity and frequency of cyber threats increasing. The way that cyber security is seen and handled has the potential to be radically altered by AI-driven tools. However, there are still issues that need to be resolved, such as the dearth of AI experts and the dangers of placing an excessive amount of reliance on AI systems. It is obvious that AI will be essential to protecting our digital infrastructure as the cyber security industry grows.

## Conflict of Interest

The author declares no conflict of interest.

## References

[1] Kamoun, F. I. (2020). AI and machine learning: A mixed blessing for cybersecurity. *Proceedings of 2020 International Symposium on Networks, Computers and Communications* (ISNCC) (pp. 1–7). IEEE.

[2] Sarker, I. H. (2021). Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science, 2*, 1-18.

[3] Muthuppalaniappan, M., Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *International Journal for Quality in Health Care 2020*, *33(1)*.

[4] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security 2021*, 105, 1–20. https://doi.org/10.1016/j.cose.2021.102248.

[5] Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Retrieved from the website: https://ssrn.com/abstract=3624487

[6] Taddeo, M. M. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence, 1(12)*, 557–560.

[7] Truong, T. C. (2020). Artificial intelligence and cybersecurity: Past, presence, and future. *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, 351–363.

[8] Ricci, J., Breitinger, F., Baggili, I. (2018). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24(1)*, 231–249. https://doi.org/10.1007/s10639-018-9765-8.
[9] Zeadally, S., Adi, E., Baig, Z., Khan, I. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 1–1. https://doi.org/10.1109/access.2020.2968045.
[10] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62(1)*, 1–16. https://doi.org/10.1080/08874417.2020.1712269.