Herodotus' Journal of the Human and Social Sciences	Volume: 9 / N°: 5 (2025), p371-386.

Applications of Artificial Intelligence in Enhancing Cybersecurity: A Study of Opportunities and Challenges

تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني: دراسة الفرص والتحديات

AHADDAD Mourad	*DJABALLAH Hakima*
University Algiers 2, Algeria	*University Algiers 3, Algeria*
mourad.ahaddad@univ-alger2.dz	*Hchenit@yahoo.fr*
https://orcid.org/0009-0000-0112-9218	*https://orcid.org/0009-0004-7109-9260*

Received 14/05/2025 *Accepted 11/12/2025*

- **Abstract:**

Cybersecurity has become a critical concern in the digital era due to the rapid growth and continuous evolution of cybercrimes, including cross-border attacks that threaten both states and individuals. Artificial intelligence (AI) plays a key role in detecting and predicting cyber threats, though it also introduces new security risks, making it a double-edged tool. This paper explores the relationship between AI and cybersecurity, focusing on the opportunities and challenges of its use, and addresses the question of how AI enhances cybersecurity. Using a descriptive methodology, the study concludes that AI can both strengthen security and increase threats, highlighting the importance of international cooperation and public awareness. The paper recommends global collaboration and increased media awareness to support cybersecurity efforts.

Keywords: Artificial Intelligence, Cybersecurity, Opportunities, Challenges, Digital Security

ملخص:

يُعدّ الأمن السيبراني من أبرز تحديات البيئة الرقمية بسبب تصاعد الجرائم الإلكترونية العابرة للحدود وتطورها المستمر مع تطور الأنظمة الشبكية، مما يستدعي تحديث آليات الحماية باستمرار. ويُعتبر الذكاء الاصطناعي أداة أساسية في كشف التهديدات السيبرانية والتنبؤ بها، رغم كونه سلاحًا ذا حدين قد يُستغل أيضًا في زيادة المخاطر. تهدف هذه الورقة إلى توضيح العلاقة بين الذكاء الاصطناعي والأمن السيبراني، واستعراض أهم الفرص والتحديات، مع الإجابة عن سؤال: كيف يساهم الذكاء الاصطناعي في تعزيز الأمن السيبراني؟ وباعتماد المنهج الوصفي، تؤكد الدراسة أهمية التوظيف الآمن للذكاء الاصطناعي، وتوصي بضرورة التعاون الدولي والتوعية الإعلامية لدعم الأمن السيبراني.

الكلمات المفتاحية :الذكاء الاصطناعي، الأمن السيبراني، الفرص، التحديات، الحماية الرقمية.

• Introduction

The rapid technological developments and the intensive use of the internet and electronic devices have led to significant transformations in cyberspace. These changes have given rise to new problems and risks that now threaten cybersecurity. Artificial intelligence (AI), with its continuous advancements, evolving applications, and numerous advantages—particularly in terms of speed and exceptional ability to detect risks before they occur—has

become one of the most relied-upon mechanisms for addressing the challenges emerging from the threats and breaches that affect individuals, institutions, and states alike. These actors are now striving to combat the growing cyberattacks and are working to protect digital information and systems by identifying threats at an early stage.

What adds to the importance of this topic is the potential misuse of AI to commit cybercrimes, as certain actors with advanced technological capabilities may exploit AI to serve personal or political agendas. This is further complicated by the difficulty of tracing digital crimes, making AI a double-edged sword—it can be used both to reinforce cybersecurity and to facilitate cyber threats.

This paper will focus on how AI technologies can be employed to achieve cybersecurity, which has become one of the most pressing concerns for institutions and states seeking to confront cybercrime and mitigate its risks. It also aims to highlight the key mechanisms through which AI contributes to cybersecurity, the opportunities it presents, and the major challenges facing its use in this field.

Given the significance of this subject, we aim to answer the following core research question:

How can the use of artificial intelligence contribute to enhancing cybersecurity, and what are the opportunities and challenges of this application in the digital environment?

This primary question is supported by the following sub-questions:

1. What is artificial intelligence, and what are its fields of application?
2. What is cybersecurity, and what are its mechanisms?
3. In what ways can AI be used to enhance cybersecurity?
4. What are the opportunities and challenges associated with this usage?

This study aims to achieve several objectives, summarized as follows:

1. Clarify the nature of artificial intelligence and its areas of application.
2. Define cybersecurity and outline its mechanisms.
3. Present the fields and applications of AI in enhancing cybersecurity.
4. Identify the opportunities and challenges of using AI in the digital environment.

The importance of this topic stems from its relevance to one of the most critical contemporary issues that concern many researchers and academic disciplines. It represents a modern field of knowledge, driven by ongoing technological advances. On the other hand, cybersecurity has become a central concern for most countries and institutions due to the rising exposure to cyber threats. AI can play a major role in reducing these risks through smart monitoring systems that enable early threat detection and rapid response. However, at the same time, AI can also contribute to the spread of cybercrime, making its use fraught with significant security challenges.

This study adopts a descriptive methodology, which aims to examine current issues in their natural context without altering them. This is achieved by collecting data on the relationship between artificial intelligence and cybersecurity and then analyzing and describing this relationship to highlight the degree of interaction and mutual influence between the two variables, as well as the challenges of AI use in the digital environment.

1. Conceptual and Theoretical Background of Artificial Intelligence

1.1 Definition of Artificial Intelligence

The role of artificial intelligence (AI) today is clearly reflected in its significant impact across various fields. Its importance is evident in modern technologies through its ability to simulate certain human functions, making it a crucial tool in many applications that require data analysis and decision-making. The concept of AI has sparked considerable debate[1].

Experts differ in its definition—some view it as a branch of computer science, while others define it as a technological evolution that gives machines human-like intelligence. So, what is meant by Artificial Intelligence?

Artificial Intelligence (AI) is the science that enables machines to make decisions and act intelligently by mimicking human thinking and behavior[2].

It is also defined as a branch of computer science that focuses on developing systems capable of processing information, learning from experiences, and adapting to change. These systems include technologies like machine learning, neural networks, and natural language processing. AI applications range from smart robotics to data management systems, all aiming to enhance user experience across various sectors. These technologies help improve efficiency, decision-making, productivity, and innovation[3].

Nelson defined AI as "the construction of machines capable of performing tasks that require human intelligence," while Elaine Rich described it as "the study of how to make computers perform tasks that humans do better"[4].

---

[1] *Amal Fawzi, Ahmed Awad* – Digital Ownership in the Age of Artificial Intelligence: Challenges of the Present and the Future – *Germany: The Arab Democratic Center for Strategic, Political, and Economic Studies, 2021, p. 6..*

[2] *Alaa Tu'ayma* – Artificial Intelligence and Its Applications in Academic Research and Publishing – *University of Al-Qadisiyah, Iraq, [no publication year], p. 7.*

[3] *Mustafa Zubair Hussein et al.* – Artificial Intelligence: Concepts and Technologies – A Scientific Guide for Students, *1st Edition – Dar Al-Sard for Printing and Publishing, Iraq, 2024, p. 13.*

[4] *Redha Abdel Jalil Ibrahim* – An Analytical Vision of Artificial Intelligence Applications and Their Role in Serving Islam – ChatGPT as a Model – *University of Sharjah, 2024, p. 7*

1.2 Historical Development of Artificial Intelligence

The origins of AI reflect humanity's early attempts to replicate human intelligence. Although research in AI dates back decades[1], its formal inception was in the 1950s—specifically in 1956—when John McCarthy and Marvin Minsky, both mathematicians, persuaded Claude Shannon (the founder of information theory) and Nathaniel Rochester (designer of IBM's first marketed computer) to organize a summer workshop at Dartmouth College[2].

The year 1956 is considered a turning point in AI's development, marking the first use of the term "Artificial Intelligence." This period attracted pioneering minds in the field. The following decades saw significant advancements in algorithm development, enhancing machines' abilities to learn and adapt. Research and development efforts helped shape AI as a field that combines computer science, mathematics, and psychology.

Despite rapid progress, AI experienced periods of stagnation known as the "AI winters"[3], characterized by declining interest and funding due to unrealistic expectations and technological limitations. However, a major shift occurred in the early 2000s with increased computing power and the availability of large datasets. Machine learning and deep learning techniques further improved AI models, leading to enhanced applications across various domains.

1.3 Importance of Artificial Intelligence

In summary, the significance of AI can be illustrated through the following key points:

- AI is expected to preserve accumulated human expertise by transferring it to intelligent machines.

- AI will allow humans to interact with machines using natural human language instead of programming languages, making technology accessible to all, including people with disabilities—previously, only specialists could interact with advanced systems.

- AI will play a crucial role in sensitive fields such as:

-Medical diagnosis and prescriptions

-Legal and professional consultations

---

[2] Stuart Russell – Human Compatible Artificial Intelligence (So That Machines Do Not Take Over the World) – Hindawi, United Kingdom, 2022, pp. 12–16..

[3] Mustafa Zubair Hussein et al. – Artificial Intelligence: Concepts and Technologies – A Scientific Guide for Students, 1st Edition – Dar Al-Sard for Printing and Publishing, Iraq, 2024, p. 14

-Interactive education

-Security and military applications

- Smart systems will support decision-making processes, offering autonomy, accuracy, and objectivity—thus reducing errors, bias, discrimination, or prejudice.

- Intelligent machines will reduce human exposure to risks and psychological stress, allowing

people to focus on more valuable and human-centric tasks.

1.4 Characteristics of Artificial Intelligence

Artificial Intelligence (AI) is distinguished by a number of key characteristics, including:

- The ability to think and perceive.
- The ability to discover and apply knowledge.
- The ability to learn and understand from past experiences.
- The ability to reuse prior experiences in new situations.
- The use of trial and error to explore different possibilities.
- The ability to respond quickly to new conditions and circumstances.
- The ability to handle complex and difficult situations.
- The ability to manage ambiguous scenarios in the absence of complete information.
- The capability to solve problems even without full data availability.
- The ability to develop, create, and comprehend visual information.
- The ability to support administrative decision-making by delivering relevant information [1] .

1.5 Fundamental Principles of Artificial Intelligence

Understanding the fundamental principles of AI is essential for grasping how intelligent systems function and are applied across various fields. Key principles include: (Source: Zoubeir, 2024, p. 17)

---

[1] Rabee Al-Hadi (March 22, 2024). *Artificial Intelligence Systems Supporting Knowledge Management Processes*. Retrieved from http://glen.kantakil.com/article/detailsAD/650

- Machine Learning: A core aspect of AI, machine learning relies on input data and utilizes algorithms to analyze these data and identify patterns or behaviors that aid in making future decisions.
- Artificial Neural Networks: These are foundational tools in AI applications. They simulate how the human brain processes information, consisting of multiple layers of interconnected neurons. This structure enables the system to receive data and extract complex patterns.
- Deep Learning Techniques: An advancement in neural networks, deep learning is used in areas such as image processing and voice recognition. It has achieved high accuracy levels and is integral to the development of expert systems, which provide advice or recommendations in fields like medicine and finance. These systems help users make more informed decisions.

To fully understand AI principles, it's also important to consider expert systems and cognitive reasoning as vital tools for analyzing information and generating solutions[1].

2. Introduction to the Concept of Cybersecurity

Cybersecurity is a modern concept closely tied to the rise of electronic crime, which has grown alongside the expansion of digital activities. The concept has evolved significantly with technological advances in communication and the increasing activity within the digital environment. These changes have given rise to new issues, most notably the need for cybersecurity.

Historically, information security focused on protecting data from theft, destruction, or forgery. In contrast, cybersecurity refers to the protection of digital data within the electronic environment.

The digital environment we live in today urgently requires robust cybersecurity—especially with the growing use of AI technologies. These technologies can provide valuable solutions to cyber threats by analyzing attacks and detecting vulnerabilities early. Recent research emphasizes the role of AI in cybersecurity, focusing on developing applications that safeguard data and systems from various types of attacks. [2]

2.1 Definition of Cybersecurity

Some of the most important definitions of cybersecurity include:

---

[1] Mustafa Hussein Zubair et al**.** – Previously cited reference*, p. 17.*

[2] Same previously cited reference, p. 73..

"Cybersecurity is a modern term that encompasses the security of information network systems, information systems, devices, and associated applications. It consists of technical and administrative measures used to prevent unauthorized use and misuse. Moreover, it is considered a strategic weapon in the hands of governments and individuals, especially as cyber warfare has become a core tactic in modern conflicts and state-level attacks."[1]

Cybersecurity involves protecting computers, networks, software applications, critical systems, and data from potential threats. Various organizations rely on cybersecurity applications to safeguard their interests and those of their clients, as well as to comply with regulatory standards. These institutions depend on cybersecurity measures to prevent unwanted intrusions, protect sensitive and critical data, and avoid any disruption of organizational activities. Essentially- cybersecurity focuses on digital defense to prevent potential breaches and detect them in time to protect institutional and customer interests.

The importance of cybersecurity lies in its role in ensuring safety in the digital environment and protecting privacy from unauthorized access. Any breach or unauthorized access to computer systems constitutes a cyberattack, which may lead to the theft, deletion, or alteration of confidential information.[2]

In this context, cybersecurity plays a vital role in safeguarding systems, networks, and software from digital attacks aimed at accessing, altering, or destroying sensitive information. Such attacks can be carried out to exploit financial resources or to disrupt the operations of competitors. Effective cybersecurity includes the early detection and swift response to cyberattacks, along with preventive measures such as:

- Regular and systematic software updates
- Frequent vulnerability assessments
- Implementation of rigorous and precise security policies and strategies to identify and address security flaws[3]

2.2 Objectives of Cybersecurity

The main objectives of cybersecurity can be summarized as follows:

- Confidentiality and Privacy: Preventing unauthorized access to information and ensuring it is available only to authorized individuals.

---

[1] Ammar Yasser Al-Babili, *Artificial Intelligence in Confronting Fake News and the Crimes of Terrorism Financing in the Cyber Environment*, Arab Administrative Development Organization, League of Arab States, Cairo, 2023, p. 255.
[2] What Is Cybersecurity?" AWS (Amazon Web Services). https://aws.amazon.com/ar/cybersecurity. Accessed April 12, 2025
[3] Cybersecurity Technologies and Future Challenges." Al Jazeera, December 4, 2023. https://www.aljazeera.net/tech/2023/12/04. Accessed [date]

- Data Integrity and Accuracy: Ensuring that data is not modified or tampered with illegally, and maintaining its accuracy and completeness.
- Availability: Ensuring that only authorized users can access and interact with the data according to established permission and security protocols.
- Communication Privacy: Protecting communications from eavesdropping, interception, or impersonation.[1]
- Business Continuity: Ensuring the continuous availability of information systems and smart technologies while protecting the confidentiality of governmental and personal data. This includes safeguarding citizens and consumers from potential internet-related threats.
- National Security and Infrastructure Protection: Enhancing the protection of information technology systems, artificial intelligence applications, and the state's vital interests, including national security and critical infrastructure. This also involves safeguarding operational technologies, including their devices, software, services, and data.[2]

2.3 Cybersecurity Mechanisms and Technologies

There are numerous mechanisms and technologies that can be relied upon to achieve cybersecurity and reduce the risks and fraudulent practices that occur within the digital environment. These mechanisms—whether legal, security-based, or media-related—operate on all levels to minimize the risks of cyber incidents and to ensure the protection and security of data stored on computers, exchanged via global information networks, and safeguarded from hacking, fraud, or extortion.
Cybersecurity measures aim to protect computers, data systems, databases, communications, and digital interactions through the following key mechanisms:

A. Electronic Protection of Programs and Data

1. Firewalls : they were first used in the early 1990s to secure networks. A firewall includes IP protocol directives with filtering rules that either allow or deny access to users. Firewalls have rapidly evolved with the advancement of information and communication technology and now play a crucial role in: user identity verification, data encryption, malware detection, preventing various forms of potential cyberattacks

---

[1] Mahmoud Al-Rashidi, *Violence in Cybercrimes: Key Issues, Protection, and Security*, Egyptian-Lebanese House, Cairo, 2011, p. 142.
[2] Ammar Yasser Al-Babili, previously cited source, p. 256.

2. Encryption : considered one of the most important methods for ensuring data confidentiality and integrity. It is a fundamental technical tool in securing electronic information. Encrypted data remains secure during exchange, and upon decryption, the recipient can confirm that the message has not been altered or tampered with. Encryption typically follows two main approaches:

a. Virtual Private Network (VPN) Approach: this method involves creating a secure tunnel between sender and receiver, where all data and messages are encrypted before being exchanged. VPNs are often used between an organization and its branches or clients.

b. Security via SSL (Secure Sockets Layer): this method allows the encryption of all data related to commercial transactions between an organization and its customers. The encryption occurs between the customer's web browser and the organization's web server. Trusted digital certificates supported by the SSL protocol enhance the reliability and security of the transaction, allowing websites to be recognized as secure and trustworthy.[1]

3.Authentication and Alert Systems: these programs monitor user permissions granted to individuals interacting with computer systems or information networks. Additionally, they are capable of issuing real-time alerts, prompting quick intervention and response to violations. This functionality helps limit damage and stop breaches promptly.

4. Biological Security:

Biometric security, such as fingerprints, voice recognition, and eye scans, is used to verify the identity of the user and prevent any unauthorized access to information systems and technological communication networks. This method is particularly useful when multiple users share the same device, ensuring that only authorized individuals can access the system.

5. Virtual Private Network (VPN):

A VPN is a private network created by an organization or entity over a public network, utilizing the infrastructure of the public network while ensuring secure communication. A VPN is typically created dynamically, activated only when needed. The network ensures the security of data transmission by encrypting the data and verifying its authenticity using secret keys known only to the parties involved in the private network.

6. Computer Network Security Systems:

These systems include security assessments aimed at identifying potential vulnerabilities in networks, which could allow unauthorized access to computers. Specialized programs are employed to detect and prevent any form of network breach or hacking attempt.

---

[1] *Abbas Lahmar,* The Strategic Dimension of Information and Communication Technology*,* Houma Publishing, Algeria, 2018, pp. 235–237..

7. Antivirus Programs:

These programs, downloaded from the internet, are essential in preventing viruses from entering the computer's memory. They help in detecting and stopping viruses if they manage to infiltrate the system. It is important to use original versions of programs and applications, as pirated or unlicensed versions may contain harmful viruses or malware.

8. Digital Signatures:

Digital signatures ensure the security of economic and financial transactions conducted over the internet. These systems utilize a set of private and public encryption keys to create a secure framework, ensuring the confidentiality and integrity of online transactions.[1]

B. Securing Internet Connectivity Operations:

The following guidelines are critical for maintaining secure internet connectivity:

- Avoid downloading programs or files from untrusted sources or unknown links.
- Do not interact with emails from unknown senders.
- Do not store sensitive information or private images on computers connected to the internet.
- Use complex passwords to enhance security.
- Avoid responding to requests made during chats or messages that seem suspicious.
- Use multiple search engines when searching for information online.
- Change your device identification number (IP address) regularly for added security.

C. Securing Data and Information on Mobile Devices:

- Set a passcode or use fingerprint recognition for accessing the device.
- Use encryption systems available on the devices to ensure data security.
- Install and regularly update antivirus protection and malware protection systems.
- Regularly back up important data.
- Avoid storing financial information on mobile devices.[2]

3. Artificial Intelligence and Enhancing Cybersecurity:

3.1 The Relationship Between Artificial Intelligence and Cybersecurity:

In the context of cybersecurity, artificial intelligence (AI) refers to systems that perform broader roles than traditional systems. AI operates similarly to human cognition by

---

[1] Mahmoud Al-Rashidi, previously cited source, pp. 143–144.

[2] Mahmoud Al-Rashidi, previously cited source, pp. 148–149.

classifying situations and prioritizing actions. In cybersecurity, AI will play a significant role in two main directions:

First Direction: AI will analyze current data, predict potential cyberattacks before they occur, and take preemptive actions. This depends heavily on the type, strength, quantity, and source of the data being analyzed.

Second Direction: AI will help identify new cyberattacks that have not been previously encountered by the system. AI's strength lies in its ability to detect unknown attacks or suspicious behavior, effectively putting them "on the radar." Unlike traditional protection systems, AI can sense cyber espionage attempts that normal cybersecurity systems may miss. AI in cybersecurity has superior capabilities in terms of speed, observation accuracy, and detecting breaches. However, AI cannot replace human expertise and judgment, especially when dealing with new and sophisticated cybercrimes.[1]

Cybercrimes related to information are often carried out using novel criminal techniques, which were previously unknown and often occur in automated data processing environments. In such cases, the data being attacked is digital pulses or electronic signals, making it a unique and specific type of crime.[2] As a result, countries and organizations are increasingly vulnerable to cyberattacks, but not all attacks succeed in achieving their goals. The use of AI-powered cybersecurity software significantly improves the detection and mitigation of these attacks, reducing their potential damage.

However, certain new cyberattacks are difficult to combat with AI, as they resemble novel viruses that lack a suitable vaccine. Research continues, focusing on improving AI's role in defending against these new threats[3] .The continuous evolution of AI technology and the advancement of cyber threats highlight the need to stay up-to-date with emerging technologies and techniques to minimize cybersecurity risks. Specifically, AI systems must evolve in line with emerging cybercrime trends.

3.2 Applications of Artificial Intelligence in Cybersecurity:

First: Use of Expert Cybersecurity Systems:

An expert system generally uses human knowledge stored in a computer to solve problems. This is a relatively modern concept that is not widely used yet but will see increasing application in the near future due to the growing threats to the cybersecurity environment. It is one of the applications in the future field of cyber AI systems, and the term cyber expert systems derives from the knowledge based on experience in the field of cybersecurity. Cyber expert systems are considered meticulously designed systems that rely on reasoning processes used by experts to solve cybersecurity issues. These systems are also used to

---

[1] Alaa Abdul-Razzaq Al-Salmi, previously cited source, pp. 38–39.

[2] Manal Hilal Al-Zahra, Information and Communication Technology, 1st ed., Dar Al-Maseera, Jordan, 2014, p. 308.

[3] Alaa Abdul-Razzaq Al-Salmi, previously cited source, p. 40.

spread knowledge about mechanisms for dealing with cybersecurity threats and can be used by non-experts to improve their capabilities in addressing cybersecurity problems.[1]

An expert system is defined as "a computer-based information system composed of interaction tools with users, usage tools, and professional expertise. The purpose of the expert system is to offer advice and solutions for problems in a specific field. The advice provided is similar to what an expert would give in that domain. The system can also solve problems or clarify how to reach a solution and provide tools to solve similar problems."[2]

This means that expert systems are among the most important applications of artificial intelligence, receiving special attention due to the significant role they play in addressing and solving various security issues. The success of expert systems depends on several key components, including:

- Expertise: This includes knowledge about the problem, theories, rules, strategies for solving different problems, and helps experts make better decisions.
- Experts: Experts have the ability to recognize problems, solve them quickly and appropriately, interpret solutions, learn from experience, and reorganize knowledge. Expert systems in cybersecurity depend on the expertise of the professionals involved.
- Transferring expertise from experts to the computer.
- Reasoning and interpretation: The system is programmed to assist in reasoning and drawing conclusions.
- Rules and regulations: Expert systems are based on rules, storing knowledge and problem-solving procedures.
- Interpretation ability: Through a subsystem called the explanation system, expert systems simulate human thinking and offer various forms of assistance similar to what an expert would provide in that field.[3]

Second: Use of Smart Weapons in Combatting Cyber Threats:

Cyber weapons represent a powerful and critical force in cybersecurity. Countries are racing to acquire them despite their high costs due to their significant capacity to destroy cyber threats. These weapons are highly capable of targeting specific goals accurately, helping to directly address cyber breaches.

"Artificial intelligence techniques have contributed to the development of cyber weapons in the security sector through enhancing digital security methods, forensic analysis tools, including speech analysis, voice recognition, identity theft detection, cyber extortion prevention, and the development of intelligence and surveillance devices that include fingerprint, eye, and voice recognition in the security investigation process. Additionally,

---

[1] Same as the previous source, p. 130.

[2] Khadija Khantit, The Expert System as a Technique of Artificial Intelligence and Its Role in Knowledge Management: A Case Study, The Economic Researcher Journal, vol. 8, no. 2, 2020, p. 387.

[3] Alaa Abdul-Razzaq Al-Salmi, previously cited source, pp. 133–135.

AI helps develop databases and information systems that simplify complex operations and facilitate the detection and prevention of criminal and terrorist plots."[1]

Cyber weapons are linked to continuous technological advancements, where new innovations make them more effective at detecting threats and reducing their harmful effects, while also helping to repel and track sudden cyberattacks. AI plays a significant role in the effectiveness of smart weapons in cybersecurity by providing:

- Learning: AI improves knowledge and understanding of cybersecurity threats and risks.
- Enhancement: AI provides structured risk analysis, reducing time and providing immediate processing opportunities.[2]

The use of smart weapons plays a major role in combating cyber threats through the use of various intelligent technical means, in addition to organizational, administrative, and legal measures that help protect electronic devices from breaches. Achieving this requires certain advantages for smart weapons:

- High flexibility in ensuring the security of information.
- Smart weapons must be designed using the latest scientific systems to prevent breaches.
- Security measures should not only focus on designing protection programs.
- Awareness training for employees is essential, including lessons, lectures, and training courses.
- Securing sites from potential breaches.
- Ensuring the latest protection methods are available.[3]

4. Opportunities and Challenges of Using Artificial Intelligence in Cybersecurity:

4.1 Opportunities Provided by Artificial Intelligence in Cybersecurity:

The use of artificial intelligence (AI) can significantly contribute to enhancing cybersecurity and improving information security. The key opportunities that AI can offer in this field can be summarized in the following points:

- Risk Prediction: AI helps anticipate potential threats by understanding and identifying possible future risks.
- Discovery of Unknown Threats: AI can map out potential threats and work to prevent them, including addressing security vulnerabilities that software providers have not yet addressed.
- Handling Massive Amounts of Data: AI can process and understand vast amounts of data, a task that is often beyond the capabilities of security experts.

---

[1] Zaman Majid Ouda, Smart Weapons and Global Security: A Study of Current and Expected Risks, Journal of Political Science, no. 67, June 2024, University of Baghdad, p. 139.

[2] Alaa Abdul-Razzaq Al-Salmi, previously cited source, pp. 159–160.

[3] Same as the previous source, pp. 174–175.

- Improved Vulnerability Management: AI helps in effectively evaluating systems and making better decisions to identify weaknesses in networks.
- Enhanced Detection and Response: AI-supported cybersecurity can detect unreliable data and respond quickly and methodically to cyber threats.
- Strengthening Overall Security Posture: AI plays a crucial role in cybersecurity by identifying security threats, managing them with intelligent and secure approaches, and adopting advanced security strategies that are quick, immediate, and capable of ensuring cybersecurity.[1]

These points highlight how AI has a substantial role in cybersecurity, allowing for the intelligent management of security threats and the creation of effective, advanced security strategies.

4.2 Challenges of Using Artificial Intelligence in Cybersecurity:

Although artificial intelligence is rapidly evolving, which is crucial for cybersecurity advancement, it faces numerous challenges. Some of the key challenges include:
Continuous Evolution of Cyber Threats: Cyber threats are growing and evolving constantly due to technological advancements, which requires staying on top of these developments and incorporating them into cybersecurity measures.
Cyberwars: As AI technology evolves rapidly, the nature of cyber warfare is also transforming, making it increasingly difficult to defend against sophisticated attacks.
Malicious Use of AI: Just as AI can be used for good, it can also be misused, making it a double-edged sword. This presents ethical and security concerns.
Legal Framework: The continuous development of AI technologies necessitates corresponding legal frameworks to keep pace with the advancements and regulate their usage.

Adopting Advanced Strategies: There is a need to adopt more advanced strategies in cybersecurity to keep up with the growing applications of AI, ensuring that these systems are secure and capable of defending against evolving threats.

These challenges emphasize that while AI provides significant opportunities, there are also substantial hurdles to overcome in terms of technology, law, and strategy. Addressing these challenges requires careful planning and continuous adaptation to new developments.

- **Conclusion :**

It can be said that artificial intelligence has become a necessity in our modern era, as the rapid developments in modern communication technologies have brought about significant

---

[1] "Artificial Intelligence in Cybersecurity." Fortinet, https://www.fortinet.com/resources/cyberglossary/Artificial-intelligence-in-cybersecurity. Accessed May 6, 2025.

changes in the cyber environment. These changes have led to the emergence of many serious problems that now threaten cybersecurity. In this context, artificial intelligence can play a significant role in addressing cyber threats and enabling their early detection in order to maintain security.

Technological advancements have also been accompanied by the evolution of new forms of threats that now endanger this environment, which has become a battleground for cyber wars that threaten the security of nations and institutions. This necessitates the adoption of appropriate security measures to confront these risks and reduce their serious consequences. Artificial intelligence is considered one of the most important tools relied upon in this field, alongside legal, regulatory, and strategic mechanisms.

Key findings include:

- There is a strong relationship between artificial intelligence and cybersecurity.
- Artificial intelligence is of paramount importance due to its many advantages, such as speed, accuracy in identifying targets, and the ability to analyze and predict risks, which enables better risk management and control.
- Artificial intelligence can contribute to achieving security, but it can also be used in attacks and threats.
- Artificial intelligence has provided many opportunities for cybersecurity.
- There are still many challenges in using artificial intelligence in the field of cybersecurity, as the topic continues to evolve, requiring constant adaptation to developments.

Key recommendations:

One of the main suggestions we can offer in this area is that the topic of artificial intelligence and its applications in cybersecurity requires coordinated efforts both locally and internationally. It is essential to develop joint strategies and policies involving various stakeholders to confront cyber threats. Furthermore, there is a need to invest in this field by encouraging scientific and academic research and benefiting from the experiences of developed countries.

- **Bibliography:**

Books

1. Al-Babli, Ammar Yasser – Artificial Intelligence in Confronting Fake News, Rumors, and Terrorism Financing Crimes in the Cyber Environment – Arab Administrative Development Organization, League of Arab States, Cairo, 2023.
2. Al-Rashidi, Mahmoud – Violence in Internet Crimes: Key Issues, Protection, and Security – Egyptian Lebanese House, Cairo, 2011.
3. Fawzi, Amal & Awad, Ahmed – Digital Ownership in the Age of Artificial Intelligence: Challenges of Reality and the Future – Germany: Arab Democratic Center for Strategic, Political, and Economic Studies, 2021.

4. Hilal Zahra, Manal – Communication and Information Technology, 1st ed. – Dar Al-Maseera, Jordan, 2014.
5. Hussein, Mustafa Zubair et al. – Artificial Intelligence: Concepts and Techniques – A Scientific Guide for Students, 1st ed. – Dar Al-Sard for Printing and Publishing, Iraq, 2024.
6. Hussein, Mustafa Zubair et al. – Artificial Intelligence: Concepts and Techniques – A Scientific Guide for Students, 1st ed. – Dar Al-Sard for Printing and Publishing, Iraq, 2024. (Duplicate entry noted)
7. Ibrahim, Reda Abdel-Jalil – An Analytical Vision of AI Applications and Their Role in Serving Islam – ChatGPT as a Model – University of Sharjah, 2024.
8. Lahmar, Abbas – The Strategic Dimension of Information and Communication Technology – Houma Publishing, Algeria, 2018.
9. Russell, Stuart – Human Compatible: Artificial Intelligence and the Problem of Control (So That Machines Don't Take Over the World) – Hindari Publishing, United Kingdom, 2022.
10. Taima, Alaa – Artificial Intelligence and Its Applications in Academic Research and Publishing – University of Al-Qadisiyah, Iraq, [no publication year listed].

Articles

11. Khantit, Khadija – The Expert System as an AI Technology and Its Role in Knowledge Management: A Case Study – The Economic Researcher Journal, Vol. 8, Issue –, 2020.
12. Odeh, Zaman Majid – Smart Weapons and Global Security: A Study of Current and Anticipated Risks – Political Science Journal, Issue 67, June 2024 – University of Baghdad.

Websites

13. Artificial Intelligence in Cybersecurity – Fortinet – Accessed on 06-05-2025.

What is Cybersecurity? – AWS – Accessed on 12-04-2025.

14. Cybersecurity Technologies and Future Challenges – Al Jazeera – Accessed on 10-04-2025.
15. Al-Hadi, Rabie – AI Systems Supporting Knowledge Management Operations (22/03/2024) – Retrieved from http://glen.kantakil.com/article/detailsAD/650