Journal of Economics and Sustainable Development
Volume: 09 / N°: 01 (2026), P:98-115
ISSN : 2661-7986 EISSN: 2773-2606

Cybersecurity in a Smart Business Environment: AI-Based Management Strategies

Djokhdem Moussa [1] [*]

[1] Faculty of Economics, Business and Management Sciences Amar Telidji University of Laghouat - Algeria-

Received:25/08/2025 ***Accepted:13/01/2026*** ***Published:01/03/2026***

Abstract:

The study aimed to identify the areas and most prominent applications of artificial intelligence used to improve cybersecurity, and to identify the challenges facing the application of artificial intelligence in cybersecurity. The research was based on reviewing and analyzing previous studies and research related to artificial intelligence technology and its role in enhancing cybersecurity. Data was collected by reviewing studies and research published in scientific journals, books, and official reports. The study concluded that artificial intelligence technologies contribute to improving the efficiency of cybersecurity strategies by predicting threats and responding quickly. The study revealed an urgent need to train and qualify human resources to understand and apply artificial intelligence technologies in the field of cybersecurity effectively. The study explained that there is a need to develop a legal and ethical framework that ensures the responsible and effective use of technology within institutions and organizations. The study recommended strengthening cyber infrastructure, training and qualifying human resources, and finally interacting with ethical and legal challenges.

Keywords: Artificial Intelligence, Cybersecurity, National Institute of Standards and Technology (NIST), Communications Networks….

[*] ***Corresponding author.***

introduction

The set of tools, procedures, and practices that protect against harm, attack, and unauthorized access to networks, devices, software, and data is collectively referred to as security. (Bhardwaj et al., 2022) The explosive growth of interconnected tools, systems, and networks makes cybersecurity even more challenging. Technological advances in the digital economy and infrastructure are exacerbating this problem, leading to a marked increase in cyberattacks with devastating consequences. Moreover, researchers document the continued evolution of adversaries with ties to nation states and criminal organizations, as well as the increasing sophistication of cyberattacks that are discovering new and intrusive ways to target even the most intelligent targets.(Chitahuri et al., 2023)As a result of this progress, cyberattacks have become more frequent, larger, and more impactful. As a result, intelligence-driven cybersecurity must be implemented to manage big data and provide dynamic defense against emerging cyberattacks. By moving toward real-time assessments, continuous monitoring, and data-driven analysis to identify, protect against, detect, respond to, and catalog cyberattacks in order to prevent future security incidents, advisory organizations such as the National Institute of Standards and Technology(NIST) also encourages the use of more proactive and adaptive approaches.(Umezawa et al., 1995).

Artificial intelligence technology represents a remarkable achievement in the Fourth Industrial Revolution, thanks to its wide applications in different areas of life. This technology has been used in the economy, industry, services, military and political sectors, in addition to its major role in enhancing cybersecurity. This is related to the public affairs of individuals and societies, as it

has been used to improve cybersecurity in different countries (Dahmani, 2023).

1.1 Research problem and its questions

With the continuous development of technology and the spread of the use of the Internet and digital technologies in all aspects of daily life, exposure to cyber threats is constantly increasing. As these threats become more complex and sophisticated, there is an urgent need to use advanced technologies such as artificial intelligence to improve cybersecurity strategies and protect vital systems and data.

Based on the above, the research problem is summarized in the following main question:

What is the role of artificial intelligence in enhancing cybersecurity?

A group of sub-questions branched off from the main question:

1. What areas is AI technology used in?
2. What are the most prominent artificial intelligence applications used to improve cybersecurity?
3. What are the challenges facing the application of artificial intelligence in cybersecurity?

1.2 Research objectives

The current research aims to achieve the following objectives:

1. Learn about the areas in which artificial intelligence technology is used.
2. Revealing the most prominent applications of artificial intelligence used to improve cybersecurity.
3. Explain the challenges facing the application of artificial intelligence in cybersecurity.

1.3 Search Terms

A. Artificial Intelligence: Artificial intelligence is a branch of computer science that focuses on designing and developing systems and programs capable of performing tasks similar to human intelligence. This field uses advanced techniques and tools that rely on the high computational capabilities of computers and information technology to create models that interact, learn, and make decisions in a manner similar to humans. Branches of artificial intelligence include image and audio classification, machine translation, as well as planning and cloning. Artificial intelligence is an essential part of modern technological innovations, and is widely used in fields such as robotics, big data analysis, and the development of artificial intelligence applications for various industries (Al-Masry, 2024).

B. Cybersecurity: Cybersecurity is a field concerned with protecting computer systems, networks, and digital information from electronic threats and cyberattacks. Cybersecurity aims to secure data and prevent, detect, and respond to security breaches and cyberattacks targeting individuals and organizations. This field includes analyzing risks, designing and implementing necessary security measures to protect data and networks, and effectively dealing with and investigating security incidents for continuous learning and improvement. Cybersecurity is considered an essential element for maintaining the confidentiality of information and ensuring the continuity of computer operations and associated communications (Al-Masry, 2024).

2. Research Methodology

The descriptive approach was used based on a review of previous studies and theoretical literature related to the subject of artificial

intelligence and cybersecurity. The research relies on reviewing and analyzing previous studies and research related to artificial intelligence technology and its role in enhancing cybersecurity. Data was collected by reviewing studies and research published in scientific journals, books and official reports. The study tools used were critical and analytical techniques to extract conclusions related to artificial intelligence applications in the field of cybersecurity.

3. Previous studies

The study aimed to:Dambe et al., 2023) titled "The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Auditing," explores how AI can improve cybersecurity and internal auditing practices. Today, organizations are facing an increasing number of sophisticated cyberattacks and are actively looking for new ways to protect their sensitive information and systems. AI has emerged as a promising solution to this challenge, as it can automate cybersecurity operations, identify and respond to threats in real-time, and provide insights into potential vulnerabilities. Additionally, AI has the potential to streamline internal auditing procedures, improve accuracy, and increase visibility into an organization's operations. This paper discusses various technologies that work in conjunction with AI to improve cybersecurity and internal auditing practices. The findings of this research suggest that AI is a powerful tool that can enhance the security postureFor the institution In a way big And guarantee Compliance For requirementsOrganizational.

The study showed thatZeadally et al., 2020) titled "Harnessing the Powers of Artificial Intelligence to Improve Cybersecurity" that over the past decade, cybersecurity has become a rapidly evolving field that has been in the news frequently due to increasing threats and ongoing efforts by hackers to outwit law enforcement. Over

time, cybercriminals have improved their methods, although their initial motivations for conducting cyberattacks have remained fairly constant. The ability of traditional cybersecurity systems to identify and stop new intrusions is diminishing. Technological advances in cryptography and artificial intelligence, particularly machine learning and deep learning, have the potential to empower cybersecurity professionals to combat dynamic threats posed by adversaries. Here, we examine how AI can enhance cybersecurity solutions by pointing out its advantages and disadvantages. We also discuss potential directions for future study as AI approaches to cybersecurity are developed across a variety of application sectors.

The study aimed to:Alhayani et al., 2021) titled "Effectiveness of artificial intelligence techniques against cyber security risks applied to IT industry" aimed to study the effectiveness of artificial intelligence techniques in alleviating cyber security concerns in Iraq. The data were collected by the researcher from IT sector workers. This study used a sample of 468 individuals, and conducted confirmatory factor analysis, discriminant validity, basic model analysis, and hypothesis evaluation. Except for the expert system, which did not show any statistically significant relationship between artificial intelligence and cyber security, the P values for all variables were found to be statistically significant. The main issues were sample size, accessibility, geographic area, and fewer variables.

A study showed thatTao et al., 2021) titled "The future of artificial intelligence in cybersecurity: A comprehensive survey" that AI in cybersecurity market map helps organizations monitor, identify, detect, and repel cyber attacks in order to maintain the privacy of their data. Increasing public awareness, technological improvements, increased intelligence and law enforcement tools,

and the volume of information collected from multiple sources have all made it imperative to use reliable and enhanced cybersecurity solutions across industries. Cyber systems with AI capabilities are driven by the increasing frequency and level of cyber attacks. The increasing number of large-scale cyber attacks around the world has made companies realize the need to secure their data. These cybercriminals are motivated by extremist, non-secular group interests, transnational information theft, rivalry between competitors, and moves to gain financial gain and discredit others. The purpose of most cyber attacks is profit.

A study found thatLi, 2018) titled "Cybersecurity Meets Artificial Intelligence: A Survey" that AI and cybersecurity have many different interdisciplinary interactions. On the one hand, AI technologies, such as deep learning, can be applied to cybersecurity to build intelligent models for malware classification, intrusion detection, and intelligent threat sensing. However, AI models will face a variety of cyber threats, which will disrupt the learning, decision-making, and sampling processes. Therefore, in order to prevent adversarial machine learning, maintain the privacy of machine learning, secure federated learning, etc., AI models require specialized defense and protection technologies in the field of cybersecurity. We study the relationship between AI and cybersecurity based on the above two factors. First, we provide an overview of current research efforts related to the use of AI to counter cyberattacks, including the use of both established deep learning solutions and traditional machine learning techniques. Then, we study the counterattacks that AI may be vulnerable to, analyze their characteristics, and classify appropriate protection strategies. Finally, we summarize the current literature on developing secure AI systems, focusing on aspects of building

encrypted neural networks and implementing secure federated deep learning.

4. Theoretical framework

4.1 Artificial Intelligence: Its Concept and Areas of Use

4.1.1 The concept of artificial intelligence

Artificial intelligence is a field that focuses on developing systems and programs that simulate human intelligence in analyzing data and making decisions. Artificial intelligence is used in a wide range of fields such as e-commerce, medicine, education, and many other fields (Dahmani, 2023).

A review of the literature on the topic of artificial intelligence reveals that there are many definitions of AI technology concepts that have been published, not only by organizations and experts in the field, but also by individuals interested in the technology (Darrar, 2019).

4.1.2 Areas of use of artificial intelligence

Artificial intelligence has many uses (Research and Information Center, 2021):

A. Artificial intelligence technology is used in various service fields such as military, industrial, technical, financial, medical and educational. Prominent applications of this technology include self-driving cars and drones, robots that operate independently and operate machines used in a variety of tasks, such as working in nuclear reactors and power plants, repairing and extending cables underground, discovering mines and other tasks in which the use of humans is replaced by smart technologies.

b. It uses intelligent computational modeling to study how the human brain recognizes familiar faces and voices, processes images, extracts useful data from them, and improves memory. The same applies to the development of electronic games such as chess and video games.

A. Motor skills, verbal control and non-linearity can be exercised through smart devices that can perform mental tasks such as industrial design research, process control and decision making.

D. It is used for language teaching, automatic understanding of written and spoken language, real-time language translation with pre-programmed answers, and many searches are collected inGoogle on computers connected to the Internet.

Artificial intelligence technology has many applications in various fields, as it is used in the military, financial, service, and industrial sectors. It can also be used in the field of education through educational platforms and programmed digital applications. Artificial intelligence technology provides many benefits; in the field of medicine, it can help doctors diagnose diseases and direct treatment more accurately, while in the field of manufacturing, it can improve production processes and increase efficiency. Robots equipped with artificial intelligence technologies enable them to perform routine tasks with high accuracy and speed. However, this technology faces some challenges and limitations in areas that require creativity and human intuition (Dahmani, 2023).

4.2 Cybersecurity: Concept and Dimensions

4.2.1 Concept of Cybersecurity

Cybersecurity is defined as the protection of communications networks, information systems, and data, including devices connected to the Internet. Cybersecurity is concerned with the

preventive measures and standards that must be followed and adhered to in order to confront threats, and reduce violations or unauthorized access (Al-Otaibi, 2020).

Jabbour (2012) described it as the activity that ensures the protection of human and financial resources related to communications and information technologies, and ensures the ability to recover from losses and damages resulting from potential risks and threats, allowing the return to normal as quickly as possible.

4.2.2 Dimensions of Cybersecurity

Cybersecurity includes military, economic, social, political and human security systems that aim to maintain stability and security from all cyber threats. Integrated security includes aspects that contribute to strengthening the cybersecurity system, and are among its most important dimensions (Mukhtar, 2023):

A. Military dimension

Cybersecurity aims to maintain the ability of military units to communicate across military networks, facilitating the exchange of information and orders. The idea of creating and deploying a network for the Internet and remote targets is a point of vulnerability, especially if it is not secure. Destruction or extortion of military databases can disrupt communications between command and military units, in addition to the risk of losing control of some weapons such as drones, guided missiles, and satellites.

B. Economic dimension

As computers are used to operate and develop industries and drive the economy, the Internet will be the basis for trade, finance and financial transactions, all of which are linked together through

computer networks to ensure cyber security, which is particularly relevant to the financial sector.

C. Social dimension

There are more than 4 billion Internet users worldwide, with more than 2.6 billion people using social networking sites. Social networking sites have the highest rates of human interaction, providing ample opportunities to share ideas and successful experiences, but they also reveal the ethics of individuals. The difficulty of controlling Internet content is not only a threat to societies, but also exposes personal information to illegal uses by external parties, which threatens social peace in countries, as a result of the loss of social cybersecurity.Dr. Political Dimension

Beyond the leaks of classified documents and privileges that often lead to diplomatic crises between countries, Russia's cyber interference in the US elections is the most important evidence of the need for cybersecurity and its importance in the political dimension.H. Legal dimension

Rapid technological development requires compliance with legislation by improving legal frameworks to deal with legal and illegal activities on the Internet, as cybercrimes are mostly considered cybercrimes. Some countries lack strict legislation to deal with these phenomena.

4.3 Artificial Intelligence Applications Used to Improve Cybersecurity

4.3.1 AI Functions in Cybersecurity

Artificial intelligence is used to improve cybersecurity through the following applications (Haddawi et al., 2023):

A. Dealing with big data

Many activities are performed on our servers, which means that large amounts of data are transferred between our customers and our infrastructure every day. These operations show the challenges that cybersecurity analysts face in examining everything and assessing potential risks. Artificial intelligence is the ideal choice to detect these threats that arise during daily activities, thanks to its ability to monitor traffic, analyze server activity accurately, and identify potential risks automatically.

b. Anticipate future threats.

The amount of data that cybersecurity analysts deal with is a challenge in predicting future threats, but AI can process large amounts of data at once, enabling early detection of malicious activity. By identifying preventive measures and potential threats, wasted time and human resources can be reduced, and it helps in staying vigilant by taking steps to protect the organization.

c. Reduce threat detection time

Detecting threats quickly is critical, with 42% of organizations reporting an increase in time-sensitive threats. At the same time, AI can scan massive amounts of data simultaneously to detect cyber threats, significantly enhancing security. According to a survey, 56% of organizations reported experiencing significant stress due to threat analysis that leaves cyber analysts overwhelmed, and 23% reported that they are unable to effectively investigate threats.D. Cost Reduction

Many organizations suffer significant financial impacts from data breaches every year, and this is something that cannot be ignored or stopped in the face of criminals. According to studies, the cost savings are as high as 80% for organizations that rely on AI technologies for their cybersecurity, with services costing $2.9

million versus $6.71 million for those who do not use these technologies.

Among the prominent technologies in the field of artificial intelligence, we find:ChatGPT, despite concerns about challenges such as racial bias and a lack of reliable standards, has significant benefits in the information security arena. ChatGPT increases productivity, assists engineers, trains employees, and enhances law enforcement. The development of ChatGPT also enhances the industry's ability to detect and respond to cyberattacks in real time, which enhances overall cybersecurity resilience. ChatGPT also offers features that help researchers combat and analyze malware, fill gaps in security knowledge, and facilitate employee training on cybersecurity. Despite the challenges that may face the use of ChatGPT, it represents an important step towards improving the security and resilience of AI-based systems.

4.4 Challenges of applying artificial intelligence in cybersecurity

Artificial intelligence faces several challenges when applied in cybersecurity, including the following (Al-Amin, 2024):

A. Integrating AI into cyber systems faces many challenges and constraints, most notably the barriers that cybercriminals rely on in the new law.

B. New technology industries represent new needs for large investments in computing skills, memory, and data centers, and contribute to the construction and maintenance of industrial technology.

A. Integrating AI into cyber is not for organizations, but the key challenges are shifting in attracting the necessary talent, capturing security data, and deploying optimal AI tools.

D. Data mining tools are the easiest of the major challenges facing organizations in advanced AI applications.

e. The use of AI by cybercriminals makes it a double-edged sword, able to be used for attacks as well as a powerful defense tool, increasing the success and effectiveness of cyberattacks.

Organizations that integrate AI into their cybersecurity systems are limiting the scope of use of the technology, while cybercriminals see unlimited flexibility in influencing the technology.

5. Conclusion

The study aimed to explore how advanced technology such as artificial intelligence can be used to enhance cybersecurity strategies. This objective was achieved through a broad systematic analysis of the available literature and previous research in the field of cybersecurity and artificial intelligence.

A comprehensive methodology including literature review was used to understand current theories and methods in the field of cybersecurity and AI applications.

The most important results of the study:

1. The study showed that AI technologies contribute to improving the efficiency of cybersecurity strategies by predicting threats and responding quickly.
2. The study revealed an urgent need to train and qualify human resources to understand and apply artificial intelligence technologies in the field of cybersecurity effectively.
3. The study showed that there is a need to develop a legal and ethical framework that ensures the responsible and effective use of technology within institutions and organizations.

Based on the results achieved, stakeholders should invest in enhancing technical infrastructure and developing policies and procedures to enable the effective application of AI in the field of cybersecurity.

Research recommendations:

1. Enhancing cyber infrastructure: Institutions and organizations must invest in improving cyber infrastructure to enable the implementation of advanced technologies such as artificial intelligence.

2. Training and qualification of human resources: Training and qualification of cybersecurity specialists should be enhanced to understand and use modern technologies effectively.

3. Dealing with ethical and legal challenges: A legal and ethical framework must be developed to ensure that AI is used in cybersecurity in a responsible and balanced manner.

Future studies:

1. Explore new AI technologies to improve cyber data analysis and faster response to threats.

2. Study the impact of artificial intelligence in improving cybersecurity predictions and reducing false responses.

3. Analyze emerging security challenges associated with new applications of AI in cybersecurity.

the reviewer

Arabic references

Al-Amin, Dabbar Muhammad, and Jamaluddin, Babu. (2024). Implications of Artificial Intelligence on National Security.Journal of Private Law, 2(1), 100-122.

Hadawi, Amira Hatem, Muslim, Dhurgham Ali, and Muhammad, Safaa Tayeh. (2023). Digital leadership and its role in enhancing cybersecurity behavior in organizations - an analytical study of the opinions of a sample of employees in private banks in Najaf. Journal of Humanities and Natural Sciences, 5(1).

Dahmani, Mohammed. (2023). Artificial Intelligence as a Mechanism to Enhance Cybersecurity. Journal of Legal and Political Thought, 7(2), 597-608.

Darar, Khadija Mohammed. Ethics of Artificial Intelligence and Robotics: An Analytical Study. International Journal of Library and Information Science, 6(3), 237-271.

Al-Otaibi, Abdulrahman Bajad Sharea. (2020). The Role of Cybersecurity in Achieving Vision 2030 (Master's Thesis). Naif Arab University for Security Sciences.

Mukhtar, Muhammad. (2023). Cybersecurity: Future Concepts, Event Trends Journal, (2), 6-7.

Research and Information Center. (2021). Artificial Intelligence. Saudi Arabia.https://www.abhacci.org.sa/ar/Centers/ResearchCenter/EServices/SouthBulletins/Documents/%D8% pdf

Al-Masry, Farah Muhammad. (2024). The Role of Artificial Intelligence in Improving Cybersecurity. Elite Journal for Studies and Research, 3(2).

Foreign references

Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93). IEEE.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access, 8, 23817-23837.

Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply to the IT industry. Materials Today: Proceedings, 531(10.1016).

Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3.

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

Bhardwaj, A., Alshehri, M.D., Kaushik, K., Alyamani, H.J., & Kumar, M. (2022). (Retracted) Secure framework against cyber attacks on cyber-physical robotic systems. Journal of Electronic Imaging, 31(6), 061802-061802.

Chithaluru, P., Al-Turjman, F., Kumar, M., & Stephan, T. (2023). Computational-intelligence-inspired adaptive opportunistic clustering approach for industrial IoT networks. IEEE Internet of Things Journal, 10(9), 7884-7892.

Umezawa, Y., Umezawa, K., & Sato, H. (1995). Selectivity coefficients for ion-selective electrodes: Recommended methods for reporting KA, Bpot values (Technical Report). Pure and applied chemistry, 67(3), 507-518.