

Cyber Artificial Intelligence: The Trilogy of Concepts, Functions, and Challenges

Ikram BELBEY *

Laboratory of Human Rights and Public Liberties
University Abdelhamid ibn badis, Mostaganem, Algeria

ikram.belbey@univ-mosta.dz

Date of submission: 10/05/2025 - Date of acceptance: 01/06/2025 - Date of publication: 29/07/2025

Abstract: This study aims to explore the importance of cyber artificial intelligence by defining its concept, functions, and challenges, while providing a future outlook on its uses. The study concludes that artificial intelligence represents a tremendous advance in technology and is a technological innovation that can significantly improve the effectiveness of cybersecurity systems. It can also be used for advanced data analysis to identify unusual behavioral patterns that may indicate cyber threats or attacks.

Keywords: Cybersecurity; Artificial Intelligence; Risks; Challenges; Future.

*Corresponding author: Ikram BELBEY

Introduction:

In recent years, we have witnessed rapid developments in technology, including advances in artificial intelligence (AI) and cybersecurity. These two technologies have radically transformed how we handle data, information, and online communication.

The use of AI in cybersecurity is becoming increasingly important, becoming an important tool for combating growing threats. AI technologies such as machine learning and big data analytics enhance organizations' defensive capabilities by analyzing user behavior and detecting abnormal patterns that may indicate potential cyberattacks.

By using these technologies, organizations can reduce their security gaps and establish more effective monitoring systems to respond to early signs of breaches. It is also worth noting that AI helps develop defense strategies that continually adapt to changing threats.

However, the application of AI in cybersecurity faces significant challenges related to ethics and privacy. Algorithms that rely on big data must be handled with caution to avoid violating individuals' privacy.

From this perspective, this study aims to examine the uses of artificial intelligence in the field of cybersecurity, and then determine its effectiveness and sufficiency in achieving its intended purpose.

In light of the above, this topic raises the following question : **Does artificial intelligence contribute positively and effectively to the field of cybersecurity?**

In light of all the above, it appears that addressing the problematic aspect of the topic, achieving its objectives, and encompassing its aspects require employing the principles of the descriptive and analytical approach. The study and analysis of this topic then focus on three axes :

I.TITLE 1 : The concept of cyber artificial intelligence

To understand the meaning of cyber AI, we must first understand the concepts of AI and cybersecurity, and then address AI in the field of cybersecurity.

First Subtitle: Artificial intelligence

Artificial intelligence (AI), sometimes called machine intelligence (MCI), is a branch of computer science and one of the cornerstones of today's technology industry. The term artificial intelligence (AI) refers to systems or devices that mimic human intelligence to perform tasks and can improve themselves based on the information they collect¹.

¹ Belassel Bint Nabi Yasmine and Amroush Al-Hussein, Artificial Intelligence and its Role in Achieving Sustainable Development, Journal of Legal and Economic Studies, Volume 5, Issue 1, 2022, p. 1155.

Cyber Artificial Intelligence: The Trilogy of Concepts, Functions, and Challenges

Despite the importance of AI in the world of technology, there is no universal, comprehensive definition of AI. It is more of a field than a concept that can be easily defined. The accepted definitions of AI vary depending on the discipline in which it developed. AI is derived from fields other than computer science, such as psychology, neuroscience, cognitive science, philosophy, linguistics, probability, and logic. Therefore, AI as a field of knowledge can be divided into several widely intersecting subfields, such as machine learning and robotics, neural networks and vision, as well as natural language processing and speech processing ¹.

As for the great jurists, Alin Turing defined it as “the ability to act as if a human being is acting by attempting to deceive the interrogator and making it appear as if a human being is answering the questions posed by the interrogator.”

John McCarthy defined it as "the science and engineering of making intelligent machines, especially", while Kurt Zewail, one of the most famous researchers in the field of artificial intelligence, defined it as "the art of making machines capable of performing operations requiring intelligence, just as humans do"².

From all of the above, artificial intelligence can be defined as "a means of controlling a computer or robot using a program that thinks in the same way as intelligent humans."

This means that artificial intelligence is a modern branch of computer science that seeks advanced methods for programming it to perform tasks and draw conclusions similar to those attributed to human intelligence. This is achieved by understanding the complex mental processes that the human mind performs during thought and translating them into equivalent computational processes that enhance the computer's ability to solve complex problems. However, this does not mean that we are faced with intelligent machines that think with the same concept of human intelligence and thinking, or that we are faced with a machine that has engaged in a type of perception or feeling comparable to the level of human perception and feeling³.

In fact, studies have shown that artificial intelligence has a special nature, as it mimics human intelligence. This is evident in several characteristics and features⁴, the most important

¹ Andersen, L, Human Rights in the Age of Artificial Intelligence, November 2018. P8.
<https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.

² Amir Farag, Civil and Criminal Liability Provisions for the Operation of Artificially Intelligent Robots for the Damages They Cause, University Press, Alexandria, 2023, p. 25.

³ Mustafa Abu Mandour Mussa Issa, The Adequacy of General Rules of Civil Liability in Compensating for Artificial Intelligence Damages: An Analytical and Comparative Study, Damietta Journal of Law and Economic Studies, Issue 5, January 2022, pp. 214-215.

⁴ In addition to the above, some of the characteristics of artificial intelligence can be added as follows:

- Artificial intelligence is used to solve problems presented in the absence of complete information.
- The ability to think, perceive, and achieve quick and effective results and conclusions.
- The ability to discover and apply knowledge within available capabilities.
- The ability to learn and understand from previous experiences and expertise.
- The ability to utilize past experiences and apply them to new situations more effectively and quickly.
- The ability to use trial and error to explore controversial issues, while increasing the ability to respond quickly to new and different situations and circumstances, as well as difficult and complex cases.
- The ability to develop, innovate, and understand and perceive visual matters.

of which is its ability to learn and perceive, and thus its independence in making certain decisions. Artificial intelligence is also characterized by accuracy and speed in some tasks¹.

While it is difficult to quantify the importance of artificial intelligence, particularly due to its continuous and rapid development, it can be highlighted in a few points, as follows:

- AI contributes to preserving accumulated human expertise by transferring it to smart machines;

- It enables humans to use human language when interacting with machines instead of computer programming languages, making the use of machines accessible to all segments of society, whereas previously, interaction with advanced machines was restricted to specialists and experts;

- AI plays an important role in many sensitive fields, such as assisting in diagnosing diseases and prescribing medications, providing legal and professional consultations, interactive education, security and military fields, and other fields;

- Intelligent systems contribute to decision-making areas. These systems are independent, accurate, and objective, and therefore their decisions are free from error, bias, racism, prejudice, or even external or personal interference;

- The application of artificial intelligence will contribute to achieving the Sustainable Development Goals; Goals 7 (Affordable and Clean Energy), 13 (Climate Action), 14 (Life Below Water) and 15 (Life on Land)².

- Artificial intelligence is already helping to build sustainable smart cities.

- AI can assist people with disabilities or special needs in multiple ways. AI is most effective in text-to-speech and speech-to-text translation, thus assisting people with visual or hearing impairments in using information and communications technology.

- Smart machines reduce human stress and risk, allowing them to focus on more important things. This can be achieved by employing these machines to perform difficult and dangerous tasks, explore unknown locations, and participate in rescue operations during natural disasters. They play an effective role in fields that involve many complex details and require intense mental focus, sustained presence of mind, and rapid, sensitive decisions that cannot tolerate delay or error, such as rapid security decisions.

- The ability to provide important information to support immediate decisions. See: Ammar Yasser Al-Babili, "The Role of Artificial Intelligence Systems in Predicting Crime," *Journal of Police Thought*, Volume 28, Issue 110, July 2019, p. 146.

¹ Belbey Ikram, *Artificial Intelligence in International Law: A Study of the Concept, Frameworks, and Applications*, Legal Book Foundation and Ibn al-Nadim Publishing and Distribution, Algeria, 2024, p. 39.

² Ahmed Al-Saleh Saba' and others., *Implementing Artificial Intelligence Strategy at the International Level (The United Arab Emirates as a Model)*, *Al-Mayadeen Economic Journal*, Volume 1, Issue 1, 2018, p. 34.

Cyber Artificial Intelligence: The Trilogy of Concepts, Functions, and Challenges

- Understanding and analyzing data and information, which is rapidly growing¹.

Second Subtitle: Cybersecurity

Cybersecurity can be defined as the combination of processes involved in protecting an individual's or organization's data online and offline. Cybersecurity is defined as "the security of networks, information systems, data, and devices connected to the internet." It therefore relates to the preventive measures and standards that must be taken and adhered to in order to address threats, prevent breaches or unauthorized access, and mitigate their impact.

It is also defined as "measures to reduce the risk of attacks on software, computers, or controls, including the means and tools used."

Based on its objectives, cybersecurity is an activity that ensures the protection of human and financial resources related to information and communications technology, the possibility of minimizing losses and damages resulting from risks and threats, and potentially enabling recovery as quickly as possible. The extent to which production is not halted and damage does not turn into loss depends on whether the activities, functions, capabilities, or information contained in information and communications systems are protected from malicious elements, use, misunderstanding, or abuse².

Third Subtitle: Artificial Intelligence in Cybersecurity

Artificial intelligence in cybersecurity is a system whose role is broader than previously recognized systems.

It thinks in a way that somewhat resembles the human mind's way of classifying and prioritizing situations. Artificial intelligence in this field will play an effective role on two main fronts in cybersecurity. The first will be through studying and analyzing existing data and working to predict attacks before they occur.

This depends largely on the type and strength of the data being analyzed, as well as its quantity and source. The second front will be through detecting new attacks that have not been previously identified in the system, but are powered by the power of artificial intelligence. Security systems can detect these attacks, or at least put them under the radar. One of the ways in which AI can detect cyber espionage attacks on countries and companies that conventional security systems cannot detect.

Cyber AI also has the potential to surpass the human mind in speed and accuracy in identifying cyber breaches, but it will never surpass human experience and knowledge. However, combining these qualities with an AI-powered system will create a bright future and revolution in cybersecurity. AI systems can also be used to analyze potential cybersecurity

¹ Belbey Ikram, op.cit, p. 48.

² Mohamed Dahmani, Artificial Intelligence as a Mechanism to Enhance Cybersecurity, Journal of Legal and Political Thought, Volume 7, Issue 2, 2023, p. 603.

implications. Using AI, the authentication framework can be more dynamic in real time and adjust access privileges based on the network and user location¹.

It's worth noting that the tools and methods currently used to protect systems and information are no longer highly effective in confronting cyber threats. This is due to their failure to keep pace with the methods used by hackers, who, in turn, strive to make the task more difficult through innovative thinking with each new technology. They also target the weakest link, the human element, and gain people's trust through social engineering.

Therefore, cybersecurity now requires adopting a defensive approach, identifying the most important attack methods, and anticipating the occurrence of these attacks. Countries and organizations may be exposed to a malicious virus that wipes out all their important files, or to a Trojan virus that enters the system voluntarily through a file or image after gaining the victim's trust. A ransomware virus encrypts all the victim's files and demands payment to decrypt the encryption, or a systematic attack that paralyzes the movement of important servers. The list goes on. Here, artificial intelligence plays a major role in identifying these attacks after they are exposed.

Many countries and organizations are exposed to cyber attacks on a near-daily basis. However, these attacks are not necessarily successful in achieving their objectives. Their reliance on cyber artificial intelligence software to prepare to counter these attacks, and identifying them correctly, clearly, and up-to-date, contributes significantly to overcoming them and reducing their damage.

However, among the most dangerous cyber attacks in cybersecurity, which AI cannot currently counter, and which often have a high success rate, are attacks that have not been previously identified by the system, and whose methods and means of countering them have not been identified. Rather, they are a loophole in a system or a completely new attack method, similar to the emergence of a new disease or virus that spreads among people and for which no vaccine or treatment has been identified.

Research and studies are ongoing in an attempt to find protection methods for such new attacks, with the current focus on the significant role AI is expected to play in repelling such attacks².

TITLE 2 : Functions and uses of artificial intelligence in the field of cybersecurity

The use of artificial intelligence (AI) in cybersecurity is becoming increasingly important as it becomes a vital tool for combating growing threats. AI technologies such as machine learning and big data analytics enhance organizations' defense capabilities by analyzing user behavior and detecting abnormal patterns that may indicate potential cyberattacks.

¹ Alaa Abdel Razzaq Al-Salmi, Introduction to Cyber Artificial Intelligence, Publications of the Arab Administrative Development Organization of the League of Arab States, Egypt, Second Edition, 2024, pp. 38-39.

² Alaa Abdel Razzaq Al-Salimi, previous reference, pp. 39-40.

Cyber Artificial Intelligence: The Trilogy of Concepts, Functions, and Challenges

First Subtitle: Positive uses of artificial intelligence in cybersecurity

This includes the use of biometric logins to create a secure login process, either by scanning fingerprints, retina scans, or handprints. This can be used alone or in conjunction with a password and is already used on most new smartphones and computers. A number of companies have been victims of security breaches, exposing email addresses, personal information, and passwords to risk. Cybersecurity experts have repeatedly stated that passwords are highly vulnerable to cyberattacks, threatening personal information, credit card information, and Social Security numbers. These are all reasons why biometric identity registration is a positive contribution of AI to cybersecurity.

AI can also be used to detect threats and other potentially malicious activity that traditional systems cannot keep up with, given the sheer number of malware created each month. Therefore, this is a potential area for AI to intervene and address this problem.

Cybersecurity companies teach AI systems to detect viruses and malware using complex algorithms that enable AI to run programs that can recognize and counter these viruses. AI systems can be trained to identify even the most subtle behaviors of malware before they enter a system and then isolate them. They can also use predictive functions that exceed the speed of traditional methods.

AI-powered systems employ rapid response strategies to keep organizations protected, using natural language processing to automatically gather information about cyberattacks. This information can provide insight into identifying anomalies that indicate cyberattacks. These preventative strategies allow cybersecurity companies to stay abreast of the latest risks and timelines and build a cyberthreat prevention strategy.

AI systems can also be used in multi-factor authentication to provide user access, allowing different corporate users to have different levels of authentication privileges, which also depend on the location from which they access data when using AI. The authentication framework can be more dynamic in real time, adjusting access privileges based on the user's network and location. Multi-factor authentication collects user information to understand that person's behavior and decide on the user's access privileges.

The use of artificial intelligence to its full potential by cybersecurity agencies in countries and companies, who are familiar with how it works to protect them from cyber threats and malware attacks, will be widespread in the near future¹.

Second Subtitle: Using artificial intelligence to detect cyber threats

AI can also be used to detect threats and other potentially malicious activities. Traditional systems cannot keep up with the sheer volume of malware being created. AI steps in and

¹ Alaa Abdel Razzaq Al-Salimi, previous reference, pp. 40-41.

addresses this problem. Cybersecurity companies teach AI systems to detect viruses and malware using complex algorithms so that AI can run pattern recognition in the software.

AI systems are also trained to identify even the most subtle behaviors of ransomware and malware attacks before they enter the system and then isolate them from the system. They can also utilize predictive functions that exceed the speed of traditional methods. AI-powered systems unlock the potential for natural language processing, which automatically gathers information based on triggers, such as articles, news, and studies about cyber threats. This information can provide insight into extreme cases, cyberattacks, and prevention strategies. This allows cybersecurity companies to stay abreast of the latest threats and develop rapid response strategies to keep organizations protected.

AI can also be used to increase network awareness. It can detect phishing by simulating clicks on email links and analyzing word choice and grammar. It can monitor network connections for the intended installation of malware, command and control communications, and the presence of suspicious packages. Furthermore, virus detection has been transformed from a solely signature-based framework, which was plagued by issues of reaction time, efficiency, and storage requirements, to behavioral analysis, which can identify unlabeled malware and previously unidentified threats¹.

TITLE 3 : Foreseeing the future of cyber artificial intelligence in light of the risks associated with its uses

Artificial intelligence technologies are essential tools in the future of information security, helping to provide solutions to growing problems as cyber threats increase and attackers' tactics become more sophisticated. The use of systems that learn from data becomes essential. However, this process can be associated with certain risks, which requires developing visions for the future of cyber AI.

First Subtitle: Risks Associated with Artificial Intelligence in Cybersecurity

The risks associated with the use of artificial intelligence in cybersecurity are important matters that require attention. AI systems improve the effectiveness of security tools, but they are complex and can be exploited by attackers. For example, machine learning algorithms can be used to create attacks that target user behavior analysis, negatively impacting information integrity. Furthermore, errors in the programming of these systems can create new security vulnerabilities, so it is important to develop security strategies that are compatible with emerging technologies.

The study of risks around artificial intelligence highlights the need to enhance transparency and accountability when designing these systems. On the other hand, evidence suggests that organizations' use of AI in cybersecurity may have negative effects. For example,

¹ Omar Yasser Al-Babili, Artificial Intelligence in the Face of Rumors and Terrorist Financing Crimes in the Cyber Environment: Implications and Responses, Publications of the Arab Administrative Development Organization, Egypt, 2023, pp. 221-222.

Cyber Artificial Intelligence: The Trilogy of Concepts, Functions, and Challenges

heavy reliance on these technologies may increase the loss of trust between users and security systems, as users may be concerned about the privacy of their data. Furthermore, AI-based software can generate misleading or biased data, impacting the reliability of the security process.

Organizations should therefore take proactive steps to train employees on how to handle these systems responsibly and reduce potential risks. Therefore, the need for research and study into the risks associated with AI technology has become a necessity.

The security use of AI requires a sound understanding of the ethical and technical issues associated with these systems. Despite the potential benefits, a deeper understanding of the risks can enhance information security and ensure the sustainability of systems. Future research should also focus on how to use AI in ways that maximize benefits, minimize harms, raise awareness, and improve policies in this field, as this is essential to creating a safer digital environment. Studies show that integrating AI into cybersecurity can improve efficiency and security.

However, the ethical and legal challenges associated with the use of AI in cybersecurity must be considered. This use raises issues around privacy and information security, as algorithms may lead to biases that influence security decisions. Therefore, measures must be taken to manage the associated risks. Frameworks must be developed to improve the ethical and security use of this technology. Balancing the benefits and risks is important to ensure information integrity and promote a culture of security¹.

Organizations also need to understand the limitations associated with using AI to analyze sensitive data, as misuse of these technologies could lead to privacy violations or unfair decision-making².

¹ Alaa Abdel Khaleq Hussein and others, *Cybersecurity: Principles and Practices to Ensure Information Integrity*, Dar Al-Sard for Printing, Publishing and Distribution, Baghdad, Iraq, First Edition, 2024, p. 123.

² It is well known that the right to privacy is a fundamental human right, guaranteed by Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. The United Nations has also issued numerous reports related to the protection of the right to privacy in light of the requirements of the digital age. In its report on the protection and promotion of privacy, it stated: "Communications technologies in the digital age have enhanced the ability of governments, institutions, and individuals to conduct surveillance, intercept communications, and collect data."

The report also emphasized the risks of big data in re-identifying "anonymized" data. The same report indicated that the burden of proving that the interference is necessary and proportionate to address the identified threat falls on the government. Therefore, mass surveillance programs can be considered arbitrary, even if they serve a legitimate purpose and are based on a legal basis. It is worth noting that the aforementioned report cited a ruling by the European Court of Human Rights, stating that the state must have the burden of ensuring that any interference with the right to privacy, family, home, or correspondence is only carried out in accordance with fully defined laws. See: Heidi Issa Hassan Ali Hassan, *Human Rights in the Age of Artificial Intelligence: Data, Insights, and Solutions*, Sharia and Law Journal, Vol. 34, No. 85, January 2021, p. 283.

AI should also be integrated into cybersecurity, but this requires addressing challenges and ethical considerations. Continued research is also required to ensure these systems are effective in mitigating risks without compromising ethical principles¹.

In accordance with current practices, a clear legislative framework should be established to guide the use of AI in this field, enhancing the compatibility of cybersecurity technology with human values.

It is also important to develop the skills of the cybersecurity workforce, so that they are prepared to meet the challenges of integrating AI and cybersecurity systems.

This field requires building a network of specialists capable of understanding the interaction of intelligent systems with information security, which will enhance protection against potential risks.

Furthermore, universities and educational institutions should develop academic programs focused on integrating AI and security practices.

Recent research has emphasized the importance of AI in improving cyber risk management, noting the need for effective assessment methods to ensure organizations' readiness and compliance with applicable standards.

Second Subtitle: The Future of Cyber Artificial Intelligence

With the increase in cyber attacks on organizations and companies in recent years, it has become clear that the current approach to cybersecurity suffers from a weak ability to combat cyber threats. Following the attacks in which Russian hackers breached a number of US government agencies, many security experts have called for a radical shift in strategies for detecting and responding to cyber threats, replacing reliance on rigid data sets with flexible artificial intelligence models capable of understanding normal, and possibly abnormal, employee behavior.

In this context, Aarti Parkar, Vice President of Security at IBM, pointed out that the increasing number of mobile devices in the workplace and the shift of companies to cloud

¹ Given the complexity of this technology and its impact on societies and humanity as a whole, UNESCO initiated a global dialogue on the ethics of artificial intelligence (AI). In September 2018, it held a public roundtable with relevant experts, followed by a global conference in March 2019, entitled "Principles of Artificial Intelligence: Towards a Humanistic Approach?" Both events aimed to raise awareness of the opportunities and challenges arising from AI and related technologies and encourage reflection.

In November 2019, the 40th session of UNESCO's General Conference intended to consider the preparation of a Recommendation on AI for the period 2020-2021, subject to approval by the UNESCO Executive Board in April 2019.

This was achieved in 2021, as the 41st session of UNESCO's General Conference, held in Paris from 9 to 24 November 2021, considered the Recommendation presented to it, which was adopted. With a holistic approach, developing it as a standard-setting instrument based on international law and focusing on human dignity and rights, as well as gender equality, social and economic justice, socioeconomic development, physical and psychological safety, diversity, interconnectedness and inclusion, and the protection of the environment and ecosystems, it can provide the necessary guidance for responsible management of AI technologies. See UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021, SHS/BIO/REC-AIETHICS/2021.

Cyber Artificial Intelligence: The Trilogy of Concepts, Functions, and Challenges

technologies have led to countless ways to access virtual workspaces, which in turn has increased the opportunities for digital breaches.

In an article published on the Fast Company website titled: The Future of Security is AI, Not Passwords, Barkar explained that this new reality requires us to redesign security systems from now on, so that they no longer rely on traditional authentication methods such as passwords, but rather resort to artificial intelligence to verify digital identities and behaviors. She pointed out that the login process should no longer be without arousal of suspicion. She added that one of the most prominent current challenges facing organizations and companies in maintaining the security of their resources and data is the blurring of the line between who can be considered part of the company's team and who is not. This is amid the increasing number of employees working remotely, ongoing integration processes, and reliance on cloud technology.

She added that in this world where user personalities are not easily distinguishable, it is not enough to be who you claim to be; your actions must also be consistent¹.

There is no doubt that the field of cybersecurity is one of the most vital fields of our time, characterized by its great dynamism in content. For example, the tools and methods adopted to protect systems and information years ago have become almost useless today, simply because this field is trying to keep up with the methods of hackers, who in turn are keen to make the task more difficult through their innovative thinking with each new technology. They also target the weakest link, the human element, and gain people's trust through social engineering.

Future cyber artificial intelligence will be systems whose role is broader than those previously recognized. They think in a manner somewhat similar to the human mind, accompanied by precision in execution when classifying situations and prioritizing.

Experts also predict that smart cyber weapons will witness significant progress in information warfare technologies, will become unstoppable, and will be difficult for their human users to control.

As cyber conflicts between countries increase in the future, identifying the parties behind them will become more difficult. It will also become more difficult to classify incidents and the parties involved. China, Russia, the United States, and other countries will enhance their capabilities to confront any smart cyber threat in the coming years by establishing new specialized cybersecurity units based on cyber artificial intelligence.

Cyber artificial intelligence technologies will be used in the future to process surveillance systems and analyze collected data. These systems will also improve information security by using them to detect and respond to cyber threats early, and to protect information systems in countries, companies, and individuals using cyber expert systems and other smart applications².

¹ Khalil Saidi and Marzouq Bin Mahdi, Artificial Intelligence as an Inevitable Trend in Cybersecurity Protection, *Journal of Human Rights Studies*, Volume 6, Issue 1, 2022, p. 35.

² Alaa Abdel Khaleq Hussein and others, previous reference, p. 124.

Conclusion:

Through the above, we have reached a set of conclusions, which we follow with the necessary recommendations as follows:

Results:

We can say that artificial intelligence represents a tremendous advancement in the field of technology, with many potential benefits and applications. However, it must be used responsibly, in accordance with laws and ethics. Emphasis must be placed on protecting privacy and avoiding the potential negative impacts of this new technology, making it an effective mechanism for achieving cybersecurity and a safer digital space.

Artificial intelligence allows for the rapid processing of vast amounts of data, enhancing organizations' ability to respond quickly to attacks. A report on the uses of artificial intelligence in cybersecurity also shows that artificial emotional intelligence can help improve interactions with patients in remote healthcare systems, opening up new ways to improve responses to psychological crises related to cybersecurity.

One of the main benefits of artificial intelligence is reducing the time required to detect threats and identify system vulnerabilities. Artificial intelligence relies on machine learning algorithms to analyze data behavior. These methods are effective in detecting unusual attack patterns that cannot be detected using traditional methods.

Recommendations:

Artificial intelligence research must continue to develop better tools to counter cyberattacks, requiring government and private institutions to invest in these areas.

Deep learning and computer vision algorithms are solutions that can help organizations detect and prevent threats before any damage occurs.

This requires expanding the applications of these technologies and integrating them with existing systems to enhance organizations' ability to counter threats.

Cybersecurity leaders should enhance their strategies by understanding how to use AI effectively.

Research efforts should be directed toward creating algorithms that analyze historical data to predict future threats, helping secure workplaces.

Legal controls, such as the General Data Protection Regulation, should be incorporated into the design and operation of AI systems to enhance cybersecurity.

Invest more funding in AI research to ensure the privacy of social media users is protected.

Promote new models of digital education and AI workforce development.

Impose penalties for AI misuse and enhance cybersecurity.