









REVIEW

AI and cybersecurity, business protection in an interconnected world: systematic literature review

IA y ciberseguridad, protección empresarial en un mundo interconectado: revisión sistemática de literatura

Iris María Cantillo Velásquez¹  , Jhon Wolfgang Echeverry David¹  , Yerlis Patricia Martínez Taborda¹  ,
Rubén Santiago Ramírez Piraquive¹  

¹Corporación Unificada Nacional de Educación Superior. Bogotá, Colombia.

Cite as: Cantillo Velásquez IM, Echeverry David JW, Martínez Taborda YP, Ramírez Piraquive RS. AI and cybersecurity, business protection in an interconnected world: systematic literature review. Management (Montevideo). 2025; 3:116. <https://doi.org/10.62486/agma2025116>

Submitted: 18-02-2024

Revised: 10-06-2024

Accepted: 04-10-2024

Published: 01-01-2025

Editor: Ing. Misael Ron 

Corresponding author: Iris María Cantillo Velásquez 

ABSTRACT

In an increasingly interconnected world, cyber threats are constantly evolving, with malicious actors developing sophisticated methods to attack enterprise systems. Traditional cybersecurity methods, such as firewalls and antivirus software, are insufficient to protect organizations from these advanced threats. A more proactive approach is needed to identify and stop threats before they cause significant damage. This research seeks to understand the current state of artificial intelligence (AI) in enterprise cybersecurity, identify best practices and methodologies for implementing effective AI solutions. To do this, the authors were based on a systematic review of the literature, adopting AI, cybersecurity, business protection and threats as fundamental categories. The search was mainly based on databases and search engines such as Scopus, Science Direct and Redalyc. The processed information was graphed through the VOSviewer software and the Lens.org platform. The usefulness and applications of AI for cybersecurity were evident. This entails the challenge of constantly updating cyber tools in order to achieve greater protection and security for users.

Keywords: Cyber Threats; Cybersecurity; Artificial Intelligence; Business Protection; Cyber Resilience; Business Systems.

RESUMEN

En un mundo cada vez más interconectado, las amenazas cibernéticas evolucionan constantemente, con actores maliciosos que desarrollan métodos sofisticados para atacar sistemas empresariales. Los métodos tradicionales de ciberseguridad, como los firewalls y el software antivirus, son insuficientes para proteger a las organizaciones de estas amenazas avanzadas. Es necesario adoptar un enfoque más proactivo que identifique y detenga las amenazas antes de que causen daños significativos. Esta investigación busca comprender el estado actual de la inteligencia artificial (IA) en la ciberseguridad empresarial, identificar las mejores prácticas y metodologías para implementar soluciones de IA efectivas. Para ello los autores se basaron en una revisión sistemática a la literatura, adoptaron como categorías fundamentales la IA, ciberseguridad, protección empresarial y amenazas. La búsqueda se basó fundamentalmente en bases de datos y buscadores como Scopus, Science Direct y Redalyc. La información procesada se graficó a través del software VOSviewer y la plataforma Lens.org. Se evidenció la utilidad y aplicaciones de la IA para la ciberseguridad. Ello conlleva el reto de actualizar de forma constante las herramientas cibernéticas con el fin de lograr mayor protección y seguridad a los usuarios.

Palabras clave: Amenazas Cibernéticas; Ciberseguridad; Inteligencia Artificial; Protección Empresarial; Resiliencia Cibernética; Sistemas Empresariales.

INTRODUCTION

In today's digital age, businesses face an increasingly complex cyber threat landscape.^(1,2,3,4,5,6,7,8) They are exposed to significant risks such as financial losses, reputational damage, and operational disruptions. The growing sophistication of cyber-attacks has outpaced the ability of traditional cybersecurity methods, such as firewalls and antivirus software, to protect business systems effectively. This highlights the need for more proactive and advanced approaches in the business and enterprise sectors.^(9,10,11,12,13,14,15,16)

A critical challenge is the shortage of cybersecurity resources and skilled personnel, which limits organizations' ability to defend themselves adequately.^(17,18,19) In addition, integrating emerging technologies, such as cloud computing and the Internet of Things (IoT), increases vulnerability and requires specific security strategies. Late detection of intrusions and the lack of effective monitoring systems exacerbate these problems, compromising business recovery and continuity.

Artificial intelligence (AI) offers a promising solution capable of analyzing large volumes of data to detect threat patterns, automating incident responses, and exploring different areas to streamline business, social, health, economic, urban, and educational processes.^(20,21,22,23,24)

However, effectively implementing AI in cybersecurity requires a deep understanding of best practices and the overcoming of technical and ethical barriers.

This article systematically reviews the literature on the use of AI in enterprise cybersecurity^(25,26,27) and explores practical applications in the functions of identifying, protecting, detecting, responding, and recovering. By analyzing opportunities and challenges, it aims to provide guidance for researchers, practitioners, and decision-makers while facilitating the adoption of AI technologies to strengthen enterprise security.

METHOD

This article presents a systematic review of AI for cybersecurity in conjunction with other literature reviews that served as the basis for this study.^(28,29,30,31,32,33,34,35,36,37,38) In addition, several articles with methodologies based on bibliometric analysis were consulted as a model for this research.^(39,40) The following phases were carried out to develop the method. First, exhaustive research was conducted on "AI for cybersecurity," using academic databases such as Scopus, Science Direct, and Redalyc, with an analysis period covering 2019-2024.

Then, a filtering and exclusion process was carried out to analyze the content, focusing on identifying thematic patterns in AI for cybersecurity. This procedure involved filtering the following areas: engineering, computing, information science, administration, and accounting. The results of this phase were represented graphically, showing the number of articles found in the different sub-areas of study.

In the third phase, some articles related to the topic were selected, their content was reviewed and analyzed, and discussions of the results were presented, considering that these systematic reviews are essential because they provide detailed information. The process was a sequence of steps that included planning and searching for information.

When searching for relevant sources in the selected databases, flexible and relevant keywords and Boolean operators were used to formulate search strings. The keywords were combined in such a way as to focus on the research interest. An analysis of the main topics identified was carried out, which was composed of the total number of publications displayed graphically. Twenty-four thousand eight hundred forty-two articles were found in the Redalyc database, 4 345 in Science Direct, and 194 in Scopus. Subsequently, based on the articles found, the context of AI in enterprise cybersecurity was analyzed and discussed, and advantages, disadvantages, opportunities, barriers, and challenges were identified.

RESULTS AND DISCUSSION

A systematic review of the literature on using artificial intelligence (AI) in enterprise cybersecurity, based on searches in Redalyc, Science Direct, and Scopus over the last five years (2019-2024), has revealed a significant volume of research. Filters applied in Administration, Engineering, Computing, and Information Sciences allowed us to identify the main trends and thematic approaches. The results are presented below in graph form. These illustrate the number of publications and their distribution by subarea, provide a detailed overview of the current research landscape, and highlight advances and areas requiring further attention.

Figure 1 shows the frequency of publications by sub-area in the period studied. Computer Science, Artificial Intelligence, Computer Security, Business, and Engineering stand out, with a frequency of over 450.



Figure 1. Table showing publication frequencies between 2019 and 2024

In this regard, the number of publications by document type increased. The number of scientific articles is particularly noteworthy, reaching a peak of 603 at the end of the first half of 2024. Figure 2 shows a graph illustrating the above.

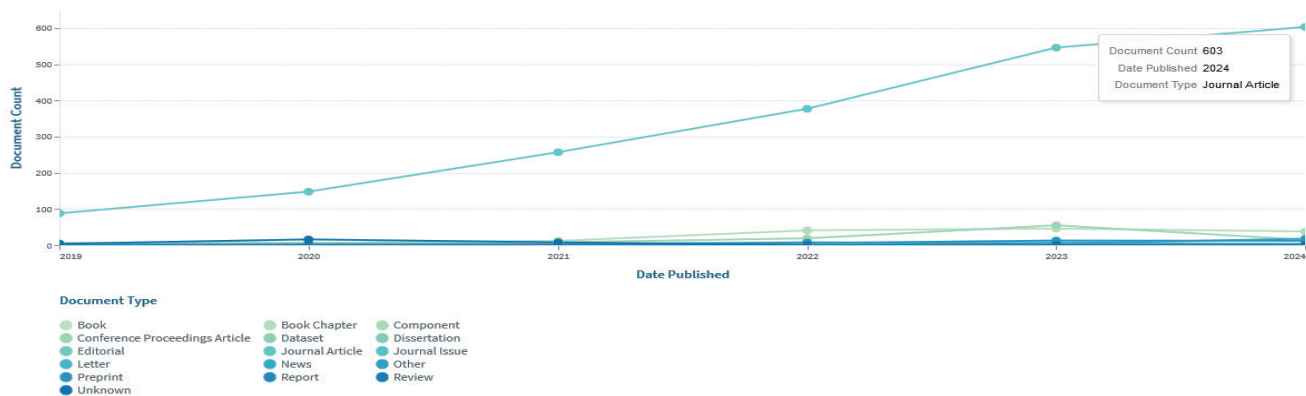


Figure 2. Types of publications between 2019 and 2024

As can be seen in figures 3 and 4, publications on AI in companies have increased exponentially compared to the years 2019-2023. In 2024, there has been growth in publications in the subareas of Administration, accounting, and Computing, which confirms that this is an emerging topic in companies. At the same time, the number of publications in Engineering has decreased.

Figure 3 shows the distribution of publications by subarea in Redalyc, highlighting the areas of Administration and Accounting (green), Engineering (orange), Computing (light blue), and Information Sciences (dark blue)).

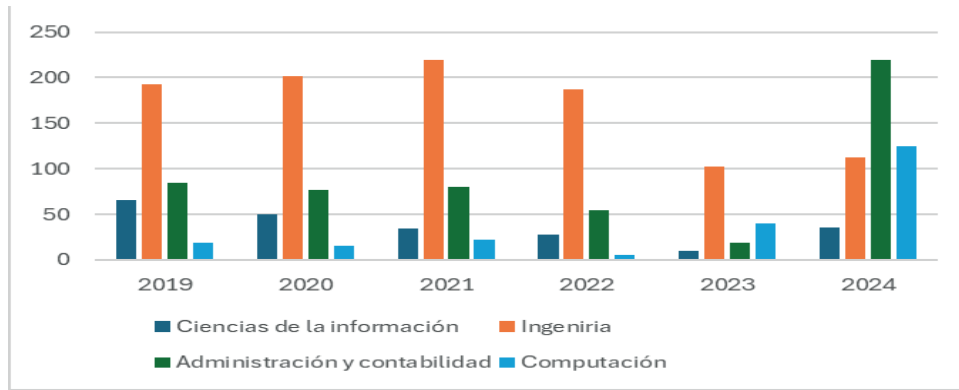


Figure 3. Literature review in Redalyc

Figure 4 shows the distribution of publications by subarea obtained through Science Direct. The relevance of each subject area can be seen, with a considerable increase in the three selected subareas. The year 2024 is affected so far because only the first semester of that year was taken into account, but its values will also rise significantly.

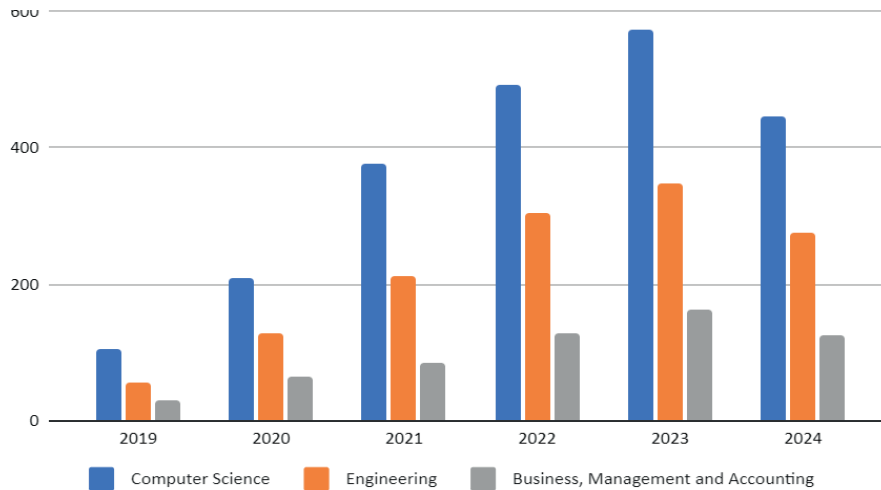


Figure 4. Literature review in Science Direct

Figure 5 illustrates the distribution of publications by subarea in Scopus, providing a comparative overview with other databases. The number of publications is lower, with a notable increase in 2023. Forecasts at the end of the first half of 2024 indicate that it will not exceed the previous year but exceed the rest of the five years.

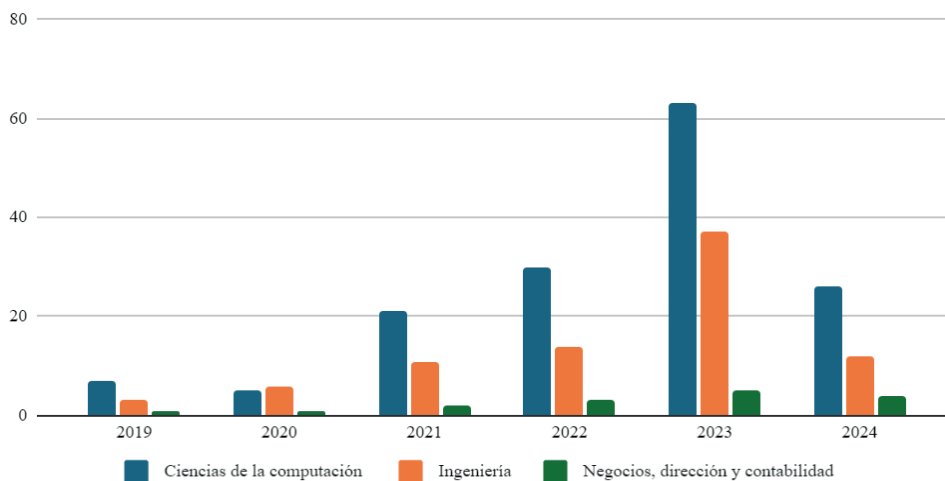


Figure 5. Literature review in Scopus

Literature review results

Within the theoretical framework for research on AI and cybersecurity in companies, it is necessary to first address the concept of cybersecurity in the context of Artificial Intelligence.⁽⁴¹⁾ Likewise, from the analysis perspective, we must comprehensively discuss the general aspects of AI-based solutions in organizational cybersecurity. Both positive and negative impacts must be considered in this analysis.^(42,43,44) We must also understand the opportunities and challenges of implementation in organizations.

In view of the above, cybersecurity protects information and communication systems connected to the Internet against malicious attacks and threats.

The Fourth Industrial Revolution and the Industrial Internet of Things (IIoT) have expanded the scope of cybersecurity from network and application security to infrastructure, cloud, and information security, making it multi-dimensional. Cybersecurity encompasses several interrelated components and technologies in cyberspace rather than being limited to system security alone. In an organizational context, cybersecurity involves simultaneously protecting all relevant dimensions of cyberspace.

“Artificial Intelligence” emerged in 1956 and has since evolved into practical solutions in various fields. The role of machine learning in cybersecurity dates back to the 1990s with the development of anomaly detection systems (ADS) and intrusion detection systems (IDS), although progress was hampered by computing and data limitations. Today, AI is an integral part of cybersecurity and transcends corporate jargon. It can simulate human intelligence and behaviors, resulting in cybersecurity automation beyond human capability, which can detect a network security breach in seconds.

The COVID-19 pandemic accelerated digital transformation and drove businesses to rely on technologies such as artificial intelligence, machine learning (ML), and big data. However, this led to an increase in cybercrime, putting individuals and established organizations at risk. Cybercrime could cost \$ 10,5 trillion by 2025. Due to their reliance on these technologies, businesses face operational and continuity risks. It is worth exploring the use of AI in cybersecurity so that organizations can understand the capabilities of AI in the cybersecurity space for the benefit of their organization.

The large amounts of data organizations generate provide opportunities for a wide range of machine learning applications in cyberspace, including threat intelligence, anomaly detection, and automation of cybersecurity-related tasks.

The relationship between AI and cybersecurity is called cyberAI

This literature review analyzes how AI can be applied in cybersecurity from an organizational perspective, the positive and negative aspects, and the opportunities and barriers to implementation.^(45,46,47) An analysis of publications on AI and cybersecurity in companies shows that AI is widely used in organizations for specific administrative and operational processes. Still, few use it to enhance cybersecurity measures and protect computers, networks, programs, and data from predators and intrusions. The statements listed here describe the different aspects of this field of research. Among the benefits of AI-driven cybersecurity are standard AI methods such as machine learning, deep learning, natural language processing, and knowledge representation and reasoning.

Other contributions include the value of AI in intelligent cybersecurity and in managing this technology, the use of combined methods, factorial and multinomial theorems, and computational methods in machine learning, cryptology, and cybersecurity. These examples demonstrate the value of mathematical and combinatorial research in increasing the importance of data analysis and security against cyberattacks.

In the modern era, organizations are concerned about cybersecurity. While projects often prioritize innovation, there is a risk of compromising cybersecurity when organizations prioritize sales features and time to market, resulting in limited risk assessments and resources allocated to cybersecurity. Strengthening the security of an organization's internal network may be insufficient, as reliance on third parties can create new avenues for cybercriminals to exploit. Therefore, organizations should consider third-party cyber risk management (C-TPRM) to mitigate these risks.^(48,49,50)

Organizations should explore new mechanisms and leverage existing cybersecurity measures. Organizations must evaluate the trade-offs between risk and reward to make informed decisions about cybersecurity investments.

Improving cybersecurity requires internal audits and controls. In addition, organizations should consider the benefits and challenges of sharing cybersecurity information. For network infrastructure, organizations typically employ local area networks (LANs) or wireless LANs for internal perimeters while using Internet access for external perimeters. In the context of Industry 4.0, where networked and wireless communications are critical, it is crucial to comply with cybersecurity guidelines and best practices.

It is essential to consider a comprehensive analysis of the challenges and strategies related to cybersecurity in mobile telecommunications networks, focusing on risk management. Among its findings are identifying specific threats such as denial-of-service (DoS) attacks, communication interceptions, and identity theft fraud.

Vulnerabilities in the telecommunications infrastructure, from base stations to end-user devices, were assessed to prioritize corrective actions. In addition, a comprehensive risk management model that encompasses identification, assessment, and mitigation based on international standards and best practices was found.

Other aspects analyzed included the implementation of technologies such as multi-factor authentication, end-to-end encryption, and artificial intelligence for incident detection and response. Recommendations were made for implementing security policies and specific training programs for mobile telecommunications networks.^(51,52)

Existing research indicates that increased cyber threats and attacks have forced organizations to adopt artificial intelligence-based technologies to safeguard their digital assets. The initial impetus for this adoption is the implementation of AI in organizational environments, and its application to cyber protection generates significant competitive advantages for organizations. Furthermore, it is believed to bring a revolutionary change in modern cyber security and scope.

The literature review found topics related to the beneficial effects of using AI in malware detection and the identification of other network or system intrusion incidents. Furthermore, AI's favorable influence extends to cybersecurity management, simplifying operational procedures and improving overall convenience.

The system can identify potential risks by identifying data patterns and detecting abnormal behavior. As a result, this automation enables organizations to take a proactive approach to recognizing, anticipating, and addressing known and unknown threats rather than relying solely on reactive measures after a cyber breach. Automating cybersecurity tasks reduces the need for human intervention, minimizes human interaction, and subsequently reduces the potential for human error throughout the security lifecycle.

Organizational cybersecurity is not just about advanced software and protection solutions. Safeguarding the physical security and vital components of hardware and infrastructure is crucial for an organization to achieve comprehensive and mature cyber protection. The multifaceted nature of artificial intelligence (AI) can have a positive impact on hardware and infrastructure security by optimizing and monitoring the data centers, servers, and processors responsible for this protection.^(53,54)

AI-powered solutions use machine learning techniques to monitor hardware temperature, cooling systems, power consumption, and backups. These solutions improve hardware performance and overall infrastructure efficiency by analyzing this data alongside historical information. In addition, implementing AI helps minimize the financial burden of hardware and infrastructure maintenance costs required to protect an organization. It does this by intelligently notifying organizations of scheduled maintenance or predicting potential failures of specific hardware components, allowing for proactive replacement before a complete breakdown occurs. Ultimately, integrating AI technologies with hardware and infrastructure maintenance can provide financial savings for organizations and reduce the overall energy consumption of hardware components.

Another positive impact of cyber AI highlighted in the reviewed literature was the scalability and interconnectivity of AI solutions at a more advanced level. Protecting the network through AI-powered network analysis systems (NAS) and network protection systems (NPS) can ensure the security and availability of computer networks within an organization, not just for a single computer but for an entire computer network system simultaneously. These AI solutions can be implemented at every stage of the security lifecycle, enabling a more comprehensive, integrated, and interconnected solution.

Although the implementation of AI in organizational cybersecurity is recognized for its ability to achieve efficiencies beyond human capabilities, several drawbacks are associated with its adoption, particularly at the organizational level.

The increased adoption of AI has led to an increase in adversarial attacks, which increases the threat of cyberattacks. The existence or absence of relevant regulations and standards can impede the adoption of AI within an organization. These adverse effects hinder or delay the widespread acceptance of AI solutions as a mainstream approach to cybersecurity. According to current literature, one of the main obstacles to the widespread adoption of AI in the cyber domain is its impact on infrastructure and hardware requirements.

Significant computing power, processing capabilities, and memory are required to effectively implement AI-driven solutions at the organizational level. In addition, larger and more advanced AI models demand modern central processing units (CPUs) that can run ten times faster than traditional processors, resulting in substantial implementation costs.

Another challenge lies in compatibility issues caused by the continued use of outdated general-purpose systems, programming languages, and technology infrastructure in many organizations. These legacy systems fail to adequately support the requirements of AI and machine learning (ML) techniques. For example, the analysis of large amounts of complex data, a critical step in successfully implementing AI and ML, is hampered by the lack of scalability offered by legacy databases and outdated systems. Implementing AI solutions in organizations is not a simple task, as it often requires a complete overhaul of the technological infrastructure.

The literature consistently highlights a recurring theme of insufficient clean, error-free, high-quality data availability. AI solutions rely on extensive data sets to train models and achieve accurate results. As a result,

obtaining a large amount of data is essential for effectively training AI models. Furthermore, implementing a cyber AI solution requires a more complex organizational data management process due to the diverse volumes and types of data stored, the speed at which they accumulate, the need to maintain data confidentiality, and the constant need for additional data. This aspect is particularly crucial because the intelligence of AI solutions depends solely on the quality of the data sets used to train the models.

There is no one-size-fits-all cyber AI solution, as most AI systems must be customized in some way for specific organizations. Although some solutions can be implemented relatively quickly, the time required to implement most cyber AI solutions at the organizational level has negatively impacted their adoption. This delay can be attributed to the inherent complexity of modern AI itself, and even the simplest AI solution can take months or even years to implement fully within an organization.

In addition to the long implementation time, it was found that implementing cyber IA presents a challenge due to its multidisciplinary nature, requiring a variety of specialized professionals such as data scientists, data analysts, artificial intelligence experts, machine learning specialists, developers, cybersecurity specialists, and project managers, each with different levels of technical expertise. It is noted that this broad need for skilled personnel poses a challenge for organizations, given the current shortage of qualified and experienced professionals in these specialized fields who can effectively implement and manage cyberIA solutions at the organizational level. Organizations often face significant financial burdens when hiring these scarce professionals.

To fully assess the impact of AI on organizational cybersecurity, it was determined that a comparison between traditional and AI-driven approaches was necessary. It was identified that there is limited literature that directly explores the difference between AI and conventional means of cyber protection. Furthermore, it is stated that each AI solution must be tailored to a specific organization and use the organization's own internal and external data. This requires greater financial, labor, and hardware and infrastructure implementation commitments than traditional approaches.

Implementing AI solutions at the organizational level is subject to stricter laws and regulations than traditional cybersecurity approaches. While AI is primarily used for defensive purposes in organizational cybersecurity, certain governments and regulatory bodies have regulated high-risk AI applications to ensure the responsible use of such powerful technology.

This study provides insights into the impact of AI on organizational cybersecurity, but it has limitations. It takes a broad view of the influence of cyber AI on organizations, overlooking variations between types, sizes, sectors, and regions of organizations, which may produce different effects. It does not delve into specific AI tools, which limits understanding of their various impacts. Time constraints limited the search for literature in other databases, potentially excluding relevant material from different sources. In addition, the inclusion/exclusion criteria limited the selection of pertinent literature, focusing on publications between 2019 and early 2024.

It should be noted that most of the existing literature in this field has focused on large, well-established organizations, so more attention needs to be paid to small and medium-sized enterprises (SMEs). Furthermore, the impacts of AI on cybersecurity identified in this review are broad and not specific to any AI-driven cybersecurity solution. Therefore, future research could explore the effects of specific AI solutions and tools on an organization's cybersecurity.

CONCLUSIONS

The existing literature highlights a growing interest in using artificial intelligence (AI) for cybersecurity, sparking ongoing debates about the effectiveness of AI methods for strengthening cybersecurity in various domains. In particular, emphasis has been placed on research into using AI for intrusion detection, improving protection, and identifying malware. As technology adoption grows within organizations, so does the emergence of cyber threats and attacks. The existing literature indicates a pressing requirement for improved and secure organizational cybersecurity methods that utilize AI-driven solutions to protect against constantly evolving threats. Therefore, this literature review research aims to analyze the overall influence of AI-driven solutions on organizational cybersecurity. The advantages and disadvantages of implementing AI-based cyber solutions in organizations were examined.

With this literature review, it was determined that the use of AI-driven solutions affects the cybersecurity of organizations throughout the security lifecycle. On the positive side, AI contributes to organizational cybersecurity by automating processes, analyzing and predicting threats, improving hardware and infrastructure security, managing vulnerabilities, assisting in decision-making, and generally improving the robustness and resilience of system security. Conversely, AI has negative implications for organizational cybersecurity. These include significant data requirements, the need for skilled professionals, hardware and infrastructure demands, implementation challenges, and the potential threat they pose to cybersecurity-related jobs. Furthermore, since hackers themselves use AI for their attacks, several of these have become resistant to AI-based protection measures. This necessitates a proactive approach to cybersecurity and introduces additional vulnerabilities

that must be considered before implementing it at the organizational level. Factors such as the absence of universal AI-based solutions and the need for stricter regulations compared to traditional cybersecurity approaches must be considered.

Despite some drawbacks, incorporating AI solutions into organizational cybersecurity has a predominantly beneficial effect. AI offers an effective, advanced, and high level of cyber protection. This result establishes a basis for future studies, which can delve deeper into specific factors such as organization size and type and assess the impact of AI. From a practical standpoint, these findings can help organizations make more informed decisions regarding AI solutions by providing an unbiased assessment of the associated effects.

REFERENCES

1. Arranz CFA, Arroyabe MF, Arranz N, de Arroyabe JCF. Digitalisation dynamics in SMEs: An approach from systems dynamics and artificial intelligence. *Technological Forecasting and Social Change*. 2023;196:122880. <https://doi.org/10.1016/j.techfore.2023.122880>
2. Cepa K, Schildt H. What to teach when we teach digital strategy? An exploration of the nascent field. *Long Range Planning*. 2023;56(2):102271. <https://doi.org/10.1016/j.lrp.2022.102271>
3. Guatemala A, Martínez G. Capacidades tecnológicas en empresas sociales emergentes: una ruta de impacto social. *Región Científica*. 2023;2(2):2023111. <https://doi.org/10.58763/rc2023111>
4. Chang V, Doan LMT, Ariel Xu Q, Hall K, Anna Wang Y, Mustafa Kamal M. Digitalization in omnichannel healthcare supply chain businesses: The role of smart wearable devices. *Journal of Business Research*. 2023;156:113369. <https://doi.org/10.1016/j.jbusres.2022.113369>
5. Dunsin D, Ghanem MC, Ouazzane K, Vassilev V. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*. 2024;48:301675. <https://doi.org/10.1016/j.fsidi.2023.301675>
6. Grosu V, Cosmulese CG, Socoliuc M, Ciubotariu M-S, Mihaila S. Testing accountants' perceptions of the digitization of the profession and profiling the future professional. *Technological Forecasting and Social Change*. 2023;193:122630. <https://doi.org/10.1016/j.techfore.2023.122630>
7. Acero AM, Ordoñez BA, Toloza HP, Vega B. Análisis estratégico para la empresa Imbocar, seccional Valledupar - Colombia. *Región Científica*. 2023;2(2):202395. <https://rc.cienciasas.org/index.php/rc/article/view/95>
8. Hanisch M, Goldsby CM, Fabian NE, Oehmichen J. Digital governance: A conceptual framework and research agenda. *Journal of Business Research*. 2023;162:113777. <https://doi.org/10.1016/j.jbusres.2023.113777>
9. Hartley N, Kunz W, Tarbit J. The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. *Organizational Dynamics*. 2024;53(2):101056. <https://doi.org/10.1016/j.orgdyn.2024.101056>
10. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business horizons*, 62(1), 15-25. <https://doi.org/10.1016/J.BUSHOR.2018.08.004>
11. Çipi A, Fernandes ACRD, Ferreira FAF, Ferreira NCMQF, Meidutė-Kavaliauskienė I. Detecting and developing new business opportunities in society 5.0 contexts: A sociotechnical approach. *Technology in Society*. 2023;73:102243. <https://doi.org/10.1016/j.techsoc.2023.102243>
12. Climent RC, Haftor DM, Staniewski MW. AI-enabled business models for competitive advantage. *Journal of Innovation & Knowledge*. 2024;9(3):100532. <https://doi.org/10.1016/j.jik.2024.100532>
13. Cosma S, Rimo G. Redefining insurance through technology: Achievements and perspectives in Insurtech. *Research in International Business and Finance*. 2024;70:102301. <https://doi.org/10.1016/j.ribaf.2024.102301>
14. Muñoz HA, Menassa IS, Rojas L, Espinosa MA. La innovación en el sector servicios y su relación compleja con la supervivencia empresarial. *Región Científica*. 2024;3(1):2024214. <https://rc.cienciasas.org/index.php/>

rc/article/view/214

15. del Val Núñez MT, de Lucas Ancillo A, Gavrilá Gavrilá S, Gómez Gandía JA. Technological transformation in HRM through knowledge and training: Innovative business decision making. *Technological Forecasting and Social Change*. 2024;200:123168. <https://doi.org/10.1016/j.techfore.2023.123168>

16. Kowalkowski C, Ulaga W. Subscription offers in business-to-business markets: Conceptualization, taxonomy, and framework for growth. *Industrial Marketing Management*. 2024;117:440-56. <https://doi.org/10.1016/j.indmarman.2024.01.014>

17. Maggie Wang Y, Matook S, Dennis AR. Unintended consequences of humanoid service robots: A case study of public service organizations. *Journal of Business Research*. 2024;174:114509. <https://doi.org/10.1016/j.jbusres.2024.114509>

18. Sarker, I. H.; Furhad, M. H.; Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, 2021, 2. <https://doi.org/10.1007/s42979-021-00557-0>

19. García M, López LS, Romero R. Control interno de inventario y la gestión de resultados de un emporio comercial de la región de San Martín - Perú. *Región Científica*. 2023;2(2):202392. <https://rc.cienciasas.org/index.php/rc/article/view/92>

20. Arroyabe MF, Arranz CFA, Fernandez De Arroyabe I, Fernandez de Arroyabe JC. Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*. 2024;78:102670. <https://doi.org/10.1016/j.techsoc.2024.102670>

21. Hoong Y, Rezania D, Baker R. When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. *Technology in Society*. 2024;78:102650. <https://doi.org/10.1016/j.techsoc.2024.102650>

22. Jada I, Mayayise TO. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*. 2024;8(2):100063. <https://doi.org/10.1016/j.dim.2023.100063>

23. Debortoli DO, Brignole NB. Inteligencia empresarial para estimular el giro comercial en el microcentro de una ciudad de tamaño intermedio. *Región Científica*. 2024;3(1):2024195. <https://doi.org/10.58763/rc2024195>

24. Ali O, Murray PA, Momin M, Dwivedi YK, Malik T. The effects of artificial intelligence applications in educational settings: Challenges and strategies. *Technological Forecasting and Social Change*. 2024;199:123076. <https://doi.org/10.1016/j.techfore.2023.123076>

25. Ghobakhloo M, Asadi S, Iranmanesh M, Foroughi B, Mubarak MF, Yadegaridehkordi E. Intelligent automation implementation and corporate sustainability performance: The enabling role of corporate social responsibility strategy. *Technology in Society*. 2023;74:102301. <https://doi.org/10.1016/j.techsoc.2023.102301>

26. Fiorentin FA, Llorca L, Suarez DV, Goren NJ. The advancement of Industry 4.0 and the transformations in the labor market Closing gender gaps? Policies under debate. *Región Científica*. 2024;3(2):2024290. <https://doi.org/10.58763/rc2024290>

27. Giordano V, Spada I, Chiarello F, Fantoni G. The impact of ChatGPT on human skills: A quantitative study on twitter data. *Technological Forecasting and Social Change*. 2024;203:123389. <https://doi.org/10.1016/j.techfore.2024.123389>

28. Gómez CA, Sánchez V, Pérez AJ. El turismo como dinamizador del desarrollo económico: una revisión mixta de la producción científica. *Dictamen Libre*. 2024;35. <https://doi.org/10.18041/2619-4244/dl.35.12114>

29. Acciarini C, Cappa F, Boccardelli P, Oriani R. How can organizations leverage big data to innovate their business models? A systematic literature review. *Technovation*. 2023;123:102713. <https://doi.org/10.1016/j.technovation.2023.102713>

30. Raudales EV, Acosta JV, Aguilar PA. Economía circular: una revisión bibliométrica y sistemática. *Región Científica*. 2024;3(1):2024192. <https://doi.org/10.58763/rc2024192>
31. Han H, Shiwakoti RK, Jarvis R, Mordi C, Botchie D. Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*. 2023;48:100598. <https://doi.org/10.1016/j.accinf.2022.100598>
32. Gómez CA, Sánchez V, Pérez AJ, Castillo W, Vitón AA, Gonzalez J. Internet of Things and Health: A literature review based on Mixed Method. *EAI Endorsed Trans IoT*. 2024;10. <https://publications.eai.eu/index.php/IoT/article/view/4909>
33. Ali O, Abdelbaki W, Shrestha A, Elbasi E, Alryalat MAA, Dwivedi YK. A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities. *Journal of Innovation & Knowledge*. 2023;8(1):100333. <https://doi.org/10.1016/j.jik.2023.100333>
34. Attard-Frost B, Brandusescu A, Lyons K. The governance of artificial intelligence in Canada: Findings and opportunities from a review of 84 AI governance initiatives. *Government Information Quarterly*. 2024;41(2):101929. <https://doi.org/10.1016/j.giq.2024.101929>
35. Velásquez LA, Paredes JA. Revisión sistemática sobre los desafíos que enfrenta el desarrollo e integración de las tecnologías digitales en el contexto escolar chileno, desde la docencia. *Región Científica*. 2024;3(1):2024226. <https://doi.org/10.58763/rc2024226>
36. Guler N, Kirshner SN, Vidgen R. A literature review of artificial intelligence research in business and management using machine learning and ChatGPT. *Data and Information Management*. 2024;8(3):100076. <https://doi.org/10.1016/j.dim.2024.100076>
37. Raman R, Pattnaik D, Hughes L, Nedungadi P. Unveiling the dynamics of AI applications: A review of reviews using scientometrics and BERTopic modeling. *Journal of Innovation & Knowledge*. 2024;9(3):100517. <https://doi.org/10.1016/j.jik.2024.100517>
38. Roppelt JS, Kanbach DK, Kraus S. Artificial intelligence in healthcare institutions: A systematic literature review on influencing factors. *Technology in Society*. 2024;76:102443. <https://doi.org/10.1016/j.techsoc.2023.102443>
39. Sánchez V, Pérez AJ, Gómez CA. Trends and evolution of Scientometric and Bibliometric research in the SCOPUS database. *Bibliotecas. Anales de Investigacion*. 2024;20(1):1-22. <http://revistas.bnjm.sld.cu/index.php/BAI/article/view/834>
40. Liao a-T, Pan C-L, Wu Z. Digital Transformation and Innovation and Business Ecosystems: A Bibliometric Analysis for Conceptual Insights and Collaborative Practices for Ecosystem Innovation. *International Journal of Innovation Studies*. 2024. <https://doi.org/10.1016/j.ijis.2024.04.003>
41. Al Dhaheri MH, Ahmad SZ, Papastathopoulos A. Do environmental turbulence, dynamic capabilities, and artificial intelligence force SMEs to be innovative? *Journal of Innovation & Knowledge*. 2024;9(3):100528. <https://doi.org/10.1016/j.jik.2024.100528>
42. Ramón A, García AD, Estrada HG. Transformaciones e impactos de la innovación financiera y el auge de las Fintech en México. *Región Científica*. 2024;3(2):2024311. <https://doi.org/10.58763/rc2024311>
43. Kumar V, Ashraf AR, Nadeem W. AI-powered marketing: What, where, and how? *International Journal of Information Management*. 2024;77:102783. <https://doi.org/10.1016/j.ijinfomgt.2024.102783>
44. Nahar S. Modeling the effects of artificial intelligence (AI)-based innovation on sustainable development goals (SDGs): Applying a system dynamics perspective in a cross-country setting. *Technological Forecasting and Social Change*. 2024;201:123203. <https://doi.org/10.1016/j.techfore.2023.123203>
45. González DIN, Garzón DP, Sánchez V. Cierre de las empresas del sector turismo en el municipio de Leticia: una caracterización de los factores implicados. *Región Científica*. 2023;2(1):202342. <https://rc.cienciasas.org/>

index.php/rc/article/view/42

46. Jiang T, Sun Z, Fu S, Lv Y. Human-AI interaction research agenda: A user-centered perspective. *Data and Information Management*. 2024;100078. <https://doi.org/10.1016/j.dim.2024.100078>

47. Sánchez RM. Classcraft: The Impact of Gamification in Higher Education. *Gamification and Augmented Reality* 2025;3:100-100. <https://doi.org/10.56294/gr2025100>.

48. Durán JFC, Paniagua RL. Water and Environmental Education: Pedagogical Field-Object in the Purépecha Indigenous Community of Naranja de Tapia, Michoacánagua. *Southern Perspective / Perspectiva Austral* 2025;3:40-40. <https://doi.org/10.56294/pa202540>.

49. Niet I, Van den Berghe L, van Est R. Societal impacts of AI integration in the EU electricity market: The Dutch case. *Technological Forecasting and Social Change*. 2023;192:122554. <https://doi.org/10.1016/j.techfore.2023.122554>

50. Papagiannidis E, Mikalef P, Conboy K, Van de Wetering R. Uncovering the dark side of AI-based decision-making: A case study in a B2B context. *Industrial Marketing Management*. 2023;115:253-65. <https://doi.org/10.1016/j.indmarman.2023.10.003>

51. Jacinto-Alvaro J, Casco RJE, Macha-Huamán R. Social networks as a tool for brand positioning. *Edu - Tech Enterprise* 2024;2:9-9. <https://doi.org/10.71459/edutech20249>.

52. Rodríguez DRD, Remon YS, Jaca SM, Domínguez AM, Gámez LGG, Borrego CEP. Biological factors of risk in those born under weight: index predictivo of the infantile mortality. *South Health and Policy* 2025;4:182-182. <https://doi.org/10.56294/shp2025182>.

53. Popkova EG, Bogoviz AV, Ekimova KV, Sergi BS. Will Russia become a blueprint for emerging nations' high-tech reforms? evidence from a 26-countries dataset. *International Journal of Innovation Studies*. 2023;7(4):294-306. <https://doi.org/10.1016/j.ijis.2023.05.001>

54. Rodgers W, Cardenas JA, Gemoets LA, Sarfi RJ. A smart grids knowledge transfer paradigm supported by experts' throughput modeling artificial intelligence algorithmic processes. *Technological Forecasting and Social Change*. 2023;190:122373. <https://doi.org/10.1016/j.techfore.2023.122373>

FINANCING

The authors did not receive funding for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David.

Data curation: Yerlis Patricia Martinez Taborda, Rubén Santiago Ramírez Piraquive.

Formal analysis: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martinez Taborda, Rubén Santiago Ramírez Piraquive.

Research: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martinez Taborda, Rubén Santiago Ramírez Piraquive.

Methodology: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David, Yerlis Patricia Martinez Taborda.

Software: Yerlis Patricia Martinez Taborda, Rubén Santiago Ramírez Piraquive.

Supervision: Iris María Cantillo Velásquez, Jhon Wolfgang Echeverry David.

Validation: Yerlis Patricia Martinez Taborda, Rubén Santiago Ramírez Piraquive.

Visualization: Yerlis Patricia Martinez Taborda, Rubén Santiago Ramírez Piraquive.

Writing - original draft: Jhon Wolfgang Echeverry David, Yerlis Patricia Martinez Taborda, Rubén Santiago Ramírez Piraquive.

Writing - review and editing: Iris María Cantillo Velásquez, Rubén Santiago Ramírez Piraquive.