Issues in Information Systems
Volume 24, Issue 4, pp. 328-338, 2023

DOI: https://doi.org/10.48009/4_iis_2023_125

Navigating the business landscape: challenges and opportunities of implementing artificial intelligence in cybersecurity governance

Rafel, Padilla-Vega, *University Ana G. Méndez, padillar1@uagm.edu*
Carlos Sanchez-Rivero, *University Ana G. Méndez, cjs@aycpr.com*
Angel Ojeda-Castro, *University Ana G. Méndez, ut_aojeda@uagm.edu*

Abstract

The term 'AI for Cybersecurity' is used to describe cybersecurity boosting measures that utilize Artificial Intelligence. At this point, removing humans from the process will hasten the process because AI can quickly explore the plethora of data sets for any potential threat. If any of these imperfections are identified, AI may utilize this information to enhance its defenses and preserve the safety of the finances and market in the business. In retail enterprises, both internal value network innovation and external value network innovation significantly contribute to the advancement of functional business model innovation and artificial intelligence business model innovation. The presence of network centrality and structural defects have the knowledge network has been linked to a positive impact on the relationship between external research and innovation. Organizations should take careful consideration of their external search strategies, considering the inverted U-shaped relationship between external search and innovation results

Keywords: artificial intelligence, cybersecurity governance, internal and external Innovations

Introduction

The infusion of Artificial Intelligence (AI) into various global industries aims to augment their income streams. Nevertheless, this cutting-edge technology demands incisive ethical scrutiny from Human Resource managers. Incorporating AI into HR practices calls for discretion by the organizational gurus to ensure distributive and procedural equity, besides preserving workplace dignity. Maintaining transparency regarding privacy policies and data collected can aid this cause. The consequences of AI and big data are potentially transformative in multiple dimensions - from ethical and economic outcomes to cultural, sustainable, and technological changes that affect the very fabric of human life. Various organizations and industries have witnessed a transformation due to AI, resulting in its penetration into human territories. However, society still has much to comprehend regarding the consequences of such swift penetration (Dwivedi et al., 2021).

The Role of Artificial Intelligence in Cybersecurity Governance: Exploring Challenges and Opportunities for Implementation

In recent times, the implementation of Artificial Intelligence (AI) in the field of cybersecurity has been progressively gaining traction, fortifying organizations against malicious threats more capably (Bhatele et al., 2019). To name a few, AI can take charge of laboriously manual constituents of core functions like identifying and resolving security risks (Bhatele et al., 2019). Resultantly, this makes the process of cyber

protection smooth, self-regulated, and uninterrupted (Bhatele et al., 2019). Additionally, AI has the potential to measure the level of vulnerability for known risks, examine massive data units to detect sophisticated attacks by adversaries, and use data for better decision-making during threat detection endeavors (Bhatele et al., 2019). AI-driven security measures have several advantages over traditional techniques, including detecting and thwarting cyber threats with minimal human intervention (Mishra, 2023).

In the financial industry, AI is employed to design robust cybersecurity protocols, mitigate the risk of unauthorized intrusion into corporate networks, and improve stakeholder participation in safeguarding data (Mishra, 2023). Furthermore, AI can enhance the effectiveness of decision-making processes (Bhatele et al., 2019). However, implementing AI-based solutions requires reliable network security measures (Mishra, 2023). In the world of cybersecurity, AI offers a multitude of benefits. However, before we can fully leverage its potential, there are several obstacles that need to be overcome, spanning legal, ethical, and technical spheres (Zhang et al., 2022). Moreover, with the proliferation of cyber-attacks and the scarcity of security experts, AI is becoming increasingly vital for businesses (Bhatele et al., 2019). The upshot of all this is that cybersecurity professionals must be able to adapt to this technological shift and hone their AI skills, as it will be a cornerstone of future security solutions (Zhang et al., 2022).

AI technology and its Growing Role in Business

Around the world, many organizations are beginning to utilize AI, a growing technology that is gaining traction. It allows machines to complete a variety of tasks that require human intelligence, such as problem-solving, learning, and decision-making (Du and Xie, 2021). This technology type is being recognized by the European Parliament which recently passed a resolution that advocated the importance of AI in the digital realm (Du and Xie, 2021). Increased revenue, enhanced security, and fast workflows are just a few of the ways that AI is utilized by businesses as it continues to progress.

As organizations begin to recognize its potential benefits, AI is increasing in prominence in the corporate sector. Sony Corp is a Japanese technological behemoth that has initiated an initiative intended to strengthen its AI business in order to ultimately make it a significant revenue source (Corvalán, 2017). However, the increase in AI employment has also led to concerns about its impact on the workforce and the necessity of obtaining new skills and training (Desouza et al., 2020). Despite these concerns, companies are supposed to continue the increased utilization of AI, with the technology having a significant role in corporate investments by the year 2025 (Desouza et al., 2020).

Businesses have many options available to them when it comes to utilizing AI. The automation of repetitive tasks, enhancements to customer service, and examining extensive data to recognize patterns and preemptive actions can all be accomplished using AI (Dwivedi et al., 2021). Now, businesses are utilizing AI in multiple areas, based on the findings of a recent study of AI conducted by McKinsey Global (Dwivedi et al., 2021). The utilization of AI is increasing steadily, and as it becomes more integral to day-to-day operations, its capacity to increase revenue and has more efficiency will only increase (Reim et al., 2020).

The Economic Considerations Associated with AI and Big Data

Big data and artificial intelligence could significantly impact the future of jobs and employment. As AI tech continues to evolve, it will enable the automation of complex processes which presently require human intervention. This shift could lead to job displacement, particularly in sectors where routine tasks can be easily automated. As highlighted in a 2022 research piece by the European Parliament, policies must be created to address the negative impact AI could have on employment. Nevertheless, AI can also result in

fresh job roles within data analytics and machine learning. It is crucial that policymakers closely examine the possible impact of AI on employment and take corrective measures to mitigate the adverse effects of these changes.

The utilization of big data and AI has the potential to worsen economic disparities and the digital divide. Inequalities in opportunity and economic prospects can be created by disparities in access to technology and proficiency in its utilization (Hernández-Fuentes, 2022). Furthermore, economic inequalities may be further exacerbated by the ownership of data and intellectual property rights related to big data and AI (Hernández-Fuentes, 2022). For this reason, it is critical to consider the ethical implications of big data and AI to guarantee that they are employed in manners that encourage fair economic results for everyone (Hernández-Fuentes, 2022).

Intellectual property and data ownership hold significant weight in the realm of AI and big data. The surge in AI technology is causing a rise in the generated and processed data that beckons ownership inquiries. There is a possibility that companies with an extensive data collection and analysis advantage may prevail over their opponents, thus raising monopolistic and unfair competition inquiries (Cabrera Diaz et al., 2021). Policymakers must acknowledge and regulate these concerns to ensure fair competition and safeguard the rights of individuals and businesses (Cabrera Diaz et al., 2021).

Future of AI in Business Innovation

Revolutionizing businesses and industries, artificial intelligence (AI) has the power to transform. Take the pandemic, for example; AI has proven to be an innovative crisis manager for organizations such as banking, leveraging the abundance of generated data (Calvo, 2020). In fashion, generative AI can potentially breed innovation in companies (Calvo, 2020). And not just that, but AI can shift the security landscape to protect individuals and establishments better alike (Calvo, 2020). Innovation opportunities arise when companies use AI to enhance their operations.

Further potential for AI can be amplified through its integration with other technologies such as big data, the Internet of Things (IoT), and blockchain. The possibilities are endless – from the development of smart cities and homes with the combination of AI and IoT to reduced fraud and improved supply chain management with the integration of AI and blockchain (Calvo, 2020). But alongside these promising breakthroughs, companies must also consider the ethical and regulatory implications that arise from AI's use. Ensuring the responsible and ethical deployment of AI is crucial given its potential impact on both society and individuals (Calvo, 2020).

AI brings plenty of opportunities to businesses, but it also presents challenges which businesses must overcome. To integrate AI effectively into operations, businesses require the necessary infrastructure and expertise to grapple with the complexity of AI implementation (Ramió, 2019). Furthermore, using intelligent systems poses potential risks, such as the possibility of bias and unintended repercussions (Ramió, 2019). Therefore, businesses need to weigh the pros and cons of AI implementation and devise a clear strategy for its usage. In summary, AI offers immense potential for business innovation, but it's necessary to consider ethical considerations and potential challenges (Ramió, 2019).

Through the lens of knowledge management theory, organizations can utilize the power of AI by utilizing knowledge-based sharing of talent and utilizing social sharing applications that are based on AI. This method provides personalized, positive experiences for employees that augment their satisfaction with their work, participate in the company, and decrease their desire to leave. This method is fueled by technology and facilitates the individual experiences of talented individuals that pursue a creative path. Innovative

cultures create a context for exchanging specific ideas regarding talent through data systems derived from insight. These concepts are then subverted into talent-based AI tools. Additionally, multinational corporations can use global talent management strategies that utilize AI to distribute knowledge effectively. Organizations that are concerned with technological advancement should consider a developed innovation strategy that involves talent management and growth, as documented in Basco et al., 2018. One method of achieving this goal is using AI and knowledge management to enhance the experience of employees while promoting innovation and achieving strategic goals, as documented in Rodriguez Alva et al., 2016.

The association between AI and company innovation can be more fully appreciated using value chain theory. The utilization of AI can facilitate a quicker decision process when recognizing, testing, and creating new solutions; this will lead to a competitive advantage (Valderrama, 2019). Design is crucial to innovation, it's involved with the process of actual decision-making, and AI-created innovations can have a positive effect on the creation of solid supply chains through information sharing, processing, and system integration (Valderrama, 2019). Implementing AI can also affect the decision-making process in supply chains; this will allow companies to have a long-term perspective and take a competitive advantage via innovation (Valderrama, 2019).

One example of an autonomous system that can have a positive impact on supply chain operations is the transportation and logistics functions (Valderrama, 2019). Implementing AI may serve as an ambiguous area for companies regarding improving their performance. However, companies can increase their performance by utilizing AI (Valderrama, 2019). Using an AI-based approach, the decision-making process in wholesale distribution can be supported, reducing the monetary loss associated with stockouts by over 56 percent (Valderrama, 2019). Companies also can alter their strategies during harmful situations and partner with their suppliers and customers via AI-assisted decision-making (Valderrama, 2019).

The enhancement of AI-based information processing abilities can facilitate long-term, sustainable supply chain innovation, despite dynamism and uncertainty (Lima, 2020). As such, supply chain managers must have AI abilities that will enhance the efficiency of supply chain metrics while also being contingent on the market's shifts and customer demands (Valderrama, 2019). Ultimately, companies can derive revenue from taking external knowledge. This leads to increased performance (Valderrama, 2019).

The cybersecurity world is also benefiting from the incredible advances in AI. With the constant nature of cyber-attacks, the necessity of using AI and machine learning to identify and prevent cyber-attacks is now apparent (Becerril Gil, 2021). By analyzing the large volume of data and risk factors, AI systems can facilitate the recognition and response to threats with a greater degree of speed and fidelity (Peña et al., 2022). Additionally, AI technology can prevent and recognize attacks before they occur, and this ultimately decreases the risk of costly data thefts (Peña et al., 2022). However, it's essential to recognize that cyber security and AI can increase or decrease one another's importance (Peña et al., 2022). As such, utilizing AI to enhance current cybersecurity practices is essential.

Companies are constantly seeking new ways to utilize artificial intelligence (AI) to their advantage in ever-evolving commercial landscapes. By doing so, they can potentially transform how businesses function. However, this also poses several challenges that must be carefully considered. Striking a balance between these opportunities and obstacles is crucial to successfully integrating AI in the business world (Du and Xie, 2021).

For companies, developing effective strategies for implementing Artificial Intelligence (AI) is of utmost importance. This involves investing in the requisite infrastructure and human resources and setting up ethical and rights-focused guidelines for the development and deployment of AI (Du and Xie, 2021).

Additionally, to keep up with the rapidly evolving tech landscape, companies must prioritize continuous learning and adaptation (Du and Xie, 2021). One of the primary roadblocks to implementing AI in businesses is the lack of knowledge and expertise in this area, which must be addressed proactively (Du and Xie, 2021). Nevertheless, the potential benefits of AI, including personalized learning and real-time feedback, make it a valuable tool for businesses to leverage (Du and Xie, 2021).

To progress the business landscape using AI, carefully weigh the advantages and drawbacks of this ever-evolving technology. Critical components of this process include creating effective implementation strategies, investing in talent and infrastructure, and continuously adapting and learning. Although there are obstacles to utilizing AI in business, the potential benefits prove it to be an invaluable asset for companies striving to maintain competitiveness on the global stage. Viewing AI as a strategy rather than a mere technology is vital, as it should guide the digital transformation process in all business areas.

Literature Review and Propositions Generation

The theoretical framework for research regarding AI and cybersecurity in companies involves utilizing AI to augment cybersecurity measures and preserve computers, networks, programs, and data from predators and invasions. The statements listed here describe the different aspects of this field of research. Sarker et al. (2021) discusses the benefits of cybersecurity driven by AI, it focuses on common AI methods like machine learning, deep learning, natural language processing, and knowledge representation and reasoning. It discusses the value of AI in the intelligent security of cyberspace and in managing this technology. Sebastio et al. (2020) discuss the utilization of combination methods, factorial theorems, and multinomial 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 safety against cyber-attacks.

Lu (2019) discusses the association between business model innovation, artificial intelligence, and the financial and market benefits of retail corporations. These examples demonstrate the positive effects of internal and external value networks regarding functional business model innovation and the benefits that it provides. (Doroshuk, 2021) specifically investigates the potential and efficacy of AI in the management of companies in the energy sector during the era of Industry 4.0. It studies the way in which AI is utilized in companies that have energy, it considers the properties and stages of development of AI. Overall, the theoretical model of research between AI and cybersecurity in organizations involves utilizing AI methods, mathematical advantages, and business model innovation to enhance cybersecurity measures, protect computers, and increase the financial and commercial benefits of organizations. These references provide crucial information regarding different aspects of the research area, they serve as a guide for future research and practical applications in the field of cybersecurity involving AI.

How AI is utilized in Cybersecurity Despite the fact that machine learning and deep learning are significant in Cybersecurity, AI is as significant. The primary objective of artificial intelligence is to succeed, even though "accuracy" is a secondary goal. The goal of dealing with difficult situations is to find creative solutions. Automated decisions are made in an actualized version of AI that takes place in the real world. It attempts to find the most effective resolution to a problem that is not simply a logical extension of the available facts. To clarify, it is important to understand the current state of AI and the specific fields that contribute to it. Highly mobile systems, especially in the cybersecurity industry, typically lack internal systems of autonomy. Most AI concepts are based on autonomous systems that are fully capable. However, it’s possible that there are currently AI systems that can assist or enhance our security services. The patterns that are observed via machine learning are beneficial for cybersecurity. These patterns are employed to

recognize and prevent dangers to the internet. It's obvious that AI lacks the capacity to interpret information as humans can. Despite attempts to move the field towards more humanlike structures, full AI is still quite distant, computers need to apply complex concepts in a variety of situations. AI is not as cutting-edge as some people would believe it to be. It's more innovative and critical.

Internal Value Network Innovation in Business

In the modern era, organizations are deeply concerned about the issue of cybersecurity (Keskin et al., 2021). While prestigious projects often prioritize innovation, there is a risk of compromising cybersecurity when organizations prioritize sales features and time-to-market, resulting in limited assessments of risk and allocated resources for cybersecurity (Heierhoff et al., 2022). Merely strengthening the security of an organization's internal network may prove insufficient, as reliance on third parties can create new avenues for cybercriminals to exploit (Keskin et al., 2021). Hence, organizations must consider the management of Cyber Third-Party Risk (C-TPRM) to mitigate these risks (Keskin et al., 2021).

In retail enterprises, both internal value network innovation and external value network innovation significantly contribute to the advancement of functional business model innovation and artificial intelligence business model innovation (Lu, 2019). The innovation of an internal value network enables enterprises to gain a deeper understanding of their internal state and redistribute internal resources to enhance their innovation capabilities (Lu, 2019). This internal value network innovation serves as a strong foundation for both functional business model innovation and artificial intelligence business model innovation (Lu, 2019) (Figure 1).

The role of business model innovation is to act as a mediator between internal value network innovation, external value network innovation, and the financial and market advantages that retail enterprises can gain (Lu, 2019). When it comes to cybersecurity, organizations should not only explore new mechanisms but also utilize existing cybersecurity measures (Heierhoff et al., 2022). To make informed decisions about cybersecurity investments, organizations should evaluate the trade-offs between risk and reward (Heierhoff et al., 2022).

Enhancing cybersecurity also requires internal auditing and controls (Haapamäki and Sihvonen, 2019). Additionally, organizations must consider the benefits and challenges associated with information sharing in cybersecurity (Haapamäki and Sihvonen, 2019). For network infrastructure, organizations typically employ local area networks (LAN) or wireless LAN for internal perimeters, while internet access is used for external perimeters (Mullet et al., 2021). In the context of Industry 4.0, where network communication and wireless communications are critical, it is crucial to adhere to cybersecurity guidelines and best practices (Mullet et al., 2021).

P1. *Artificial Intelligence has a positive impact on Internal Value Network Innovation*.

External Value Network Innovation in Business

Considering the effects of cybersecurity on innovation in an external value network (Figure 1), it is crucial to weigh the advantages and disadvantages of partnering with external search engines. Various studies have shown a connection between external search methods and the outcomes of collaborative innovation networks (Shi et al., 2020). These inquiries imply that the range and depth of external search correlate with the level of innovation. Simply put, there is an optimal threshold of external research that yields positive innovation outcomes. (Shi et al., 2020) found that surpassing a certain point of external searches can hinder

innovation results. Furthermore, the involvement of companies in knowledge networks plays a vital role in the correlation between external research and innovation outcomes.

The level of embedding of knowledge networks can also influence the effectiveness of external search tactics in relation to innovation results. Organizations must exercise caution in managing external partners and sharing information to ensure the safety of their cybersecurity. The presence of network centrality and structural defects in the knowledge network has been linked to a positive impact on the relationship between external research and innovation. While external search and collaboration can bring benefits in terms of knowledge and resources, it also opens vulnerabilities in terms of cybersecurity.

To safeguard their networks and sensitive data while collaborating with other organizations, it is imperative for organizations to implement extensive cybersecurity protocols (Shi et al., 2020); (Ramirez et al., 2018). Moreover, organizations should consider the intermediary role of product and organizational innovation in the interaction between external information and marketing innovation (Ramirez et al., 2018). The development of new marketing strategies can be greatly affected by information from sources outside the organization, such as interactions with customers, suppliers, and competitors (Ramirez et al., 2018). The level of innovation within the product and organization plays a role in influencing this information (Ramirez et al., 2018). To effectively utilize external information for marketing innovation, organizations should prioritize the building of robust capabilities in product and organizational innovation (Ramirez et al., 2018).

P2. *Artificial Intelligence has a positive impact on External Value Network Innovation.*

Finances and Market in Business

AI and cybersecurity have significant impacts on financial and entrepreneurial results in the real world (Figure 1). The combination of multiple techniques, such as binomial coefficients, factorials, and multinomial calculations, is crucial to machine learning and cryptology for the analysis of data and the creation of AI-based cybersecurity (Sebastio et al., 2020). These methods help contribute to the development of computational methods and cryptographic methods that enhance the safety of computers, devices, networks, programs, and data during cyber-attacks (Sebastio et al., 2020).

In terms of business management and innovation, both internal and external value networks have a positive effect on functional business model innovation and AI-based business model innovation in retail companies (Lu, 2019). These improvements, in turn, have a significant positive impact on the financial and commercial benefits of retail companies (Lu, 2019). The values of the internal and external innovation networks in relation to business model innovation have been documented as 0.413 and 0.258, respectively (Lu, 2019).

The utilization of AI in financial and related activities is also becoming more common. The integration of AI into financial management systems for enterprises can reduce costs, increase profits, and produce processes that are low-cost and profitable (Wang and Nor, 2022). Additionally, the integration of AI into financial accounting models based on knowledge graphs facilitates information sharing and enhances the auditing function of companies (Zhou et al., 2020). These advances help to develop intelligent financial accounting models that facilitate efficient decision-making and enhance the integration of business and finances (Zhou et al., 2020).

In the context of cybersecurity, the combination of AI and the Internet of Things (IoT) has both benefits and drawbacks, particularly in the power generation and distribution industry (Soori et al., 2023). AI has the potential to enhance the safety of cyberspace in power systems, but the full potential and effective solutions are still developing (Soori et al., 2023). Additionally, AI has a significant role in the development

of banking and financial services. This role is enabled by the ability to reduce risk, price predictions, trend analysis, portfolio creation, and detection of fraud (Sunarta and Astuti, 2023). The significance of cybersecurity in the financial sector is not exaggerated. Cybersecurity measures are crucial to preventing illegal data usage and protecting computers, software, and information from internal and external predators (Rathore et al., 2017). Breaches in cybersecurity can have significant consequences for businesses, including lower performance, decreased value, increased risk, and loss of information (Rathore et al., 2017).

> ***P3***. *Artificial Intelligence in Internal Value Network Innovation Cybersecurity has a significant implication for Finances and the Market in Business.*
>
> ***P4***. *Artificial Intelligence in External Value Network Innovation Cybersecurity has a significant implication for Finances and the Market in Business.*

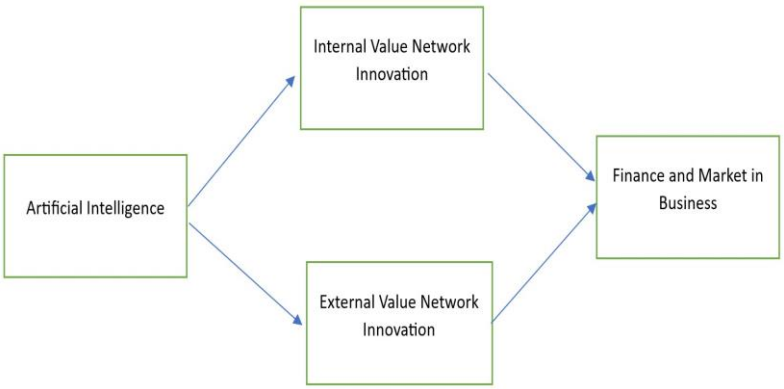

Figure 1: AI in Cybersecurity Proposed Framework

Conclusion

Cybersecurity should be a concern when collaborating with other organizations in a virtual space. Organizations should take careful consideration of their external search strategies, considering the inverted U-shaped relationship between external search and innovation results. The company's embeddedness in knowledge networks also has a significant impact on the effectiveness of external search strategies. Additionally, organizations should consider the middle-range role of products and organizational innovation in the communication between external sources and marketing innovations.

By taking proactive measures to protect their networks and information is still possible, organizations can augment their innovation results while maintaining their privacy. The combination of AI and cybersecurity has significant effects on financial and market performance in companies. Combinatorial methods, AI-based innovations, and intelligent financial accounting have the potential to enhance data analysis, administration of business, and financial management. However, it's essential to address the issues and dangers associated with cybersecurity in order to ensure the safety of computers, networks, and personal information.

AI and cybersecurity have significant impacts on financial and entrepreneurial results in the real world. AI has a significant role in the development of banking and financial services. It enables the reduction of risk,

the anticipation of prices, the analysis of trends, the creation of portfolios, and fraud detection. The significance of cybersecurity in the financial sector is not exaggerated.

References

Basco, A. I., Beliz, G., Coatz, D., & Garnero, P. (2018). Industria 4.0: Fabricando el futuro (Vol. 647). Inter-American Development Bank.

Becerril Gil, A. A. (2021). Retos para la regulación jurídica de la inteligencia artificial en el ámbito de la ciberseguridad. Revista IUS, 15(48), 9–34.

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In Countering cyber-attacks and preserving the integrity and availability of critical systems (pp. 170–192). IGI Global.

Cabrera Diaz, D., et al. (2021). La competencia desleal y el aumento de este tipo de prácticas debido al uso de redes sociales.

Calvo, J. (2020). Viaje al futuro de la empresa. Cómo competir en la era del liderazgo moonshot y las Organizaciones Exponenciales. Libros de Cabecera, SL.

Corvalán, J. G. (2017). Administración pública digital e inteligente: Transformaciones en la era de la inteligencia artificial. Revista de Direito Econômico e Socioambiental, 8(2), 26–66.

Desouza, K. C., Dawson, G. S., & Chenok, D. (2020). Designing, developing, and deploying artificial intelligence systems: Lessons from and for the public sector. Business Horizons, 63(2), 205–213.

Doroshuk, H. (2021). Prospects and efficiency measurement of artificial intelligence in the management of enterprises in the energy sector in the era of industry 4.0. Polityka Energetyczna, 24(4), 61–76.

Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities. Journal of Business Research, 129, 961–974.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., et al. (2021). Artificial intelligence (ai): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. Managerial Auditing Journal, 34(7), 808–834.

Heierhoff, S., Reher, A., & Slamka, J. (2022). The impact of the organizational design of innovation units on the consideration of cybersecurity.

Hernández-Fuentes, A. P. (2022). Cooperación digital y soberanıa tecnológica para cerrar la brecha digital en la cuarta revolución industrial. Oasis, (36), 77–94.

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. Electronics, 10(10), 1168.

Lima, C. (2020). Hoja de ruta para implementación de la transformación digital en empresas tradicionales de grande porte.

Lu, Y. (2019). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1–29.

Mishra, S. (2023). Exploring the impact of ai-based cyber security financial sector management. Applied Sciences, 13(10), 5875.

Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access, 9, 23235– 23263.

Peña, R. S., Fernández, L. F. Z., Rodrıguez, A. M. G., Urrutia, Y. C., & Zamora,Y. M. (2022). Sistema de recomendaciones en la mejora de procesos de software aplicando técnicas de inteligencia artificial. Serie Cientıfica de la Universidad de las Ciencias Informáticas, 15(6), 1–17.

Ramió, C. (2019). Inteligencia artificial y administración pública: Robots y humanos compartiendo el servicio público. Los libros de la Catarata.

Ramirez, F. J., Parra-Requena, G., Ruiz-Ortega, M. J., & Garcia-Villaverde, P. M. (2018). From external information to marketing innovation: The mediating role of product and organizational innovation. Journal of Business & Industrial Marketing, 33(5), 693–705.

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. Information sciences, 421, 43–69.

Reim, W., Åström, J., & Eriksson, O. (2020). Implementation of artificial intelligence (ai): A roadmap for business model innovation. AI, 1(2), 11.

Rodriguez Alva, J. P., Ortiz Puente de la Vega, J. H., Vera Zavala, G. E., Soto Carpio, J. J., & Delgado Palomino, J. A. (2016). Satisfaccion y rotacion laboral en personal de empresas mineras de arequipa y cusco.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2, 1–18.

Sebastio, S., Baranov, E., Biondi, F., Decourbe, O., Given-Wilson, T., Legay, A., Puodzius, C., & Quilbeuf, J. (2020). Optimizing symbolic execution for malware behavior classification. Computers & Security, 93, 101775.

Shi, X., Zheng, Z., Zhang, Q., & Liang, H. (2020). External knowledge search and firms' incremental innovation capability: The joint moderating effect of technological proximity and network embeddedness. Management Decision, 58(9), 2049–2072.

Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. Internet of Things and Cyber-Physical Systems.

Sunarta, I. N., & Astuti, P. D. (2023). Accounting information system quality and organizational performance: The mediating role of accounting information quality. International Journal of Professional Business Review, 8(3), e01192–e01192.

Valderrama, B. (2019). Transformación digital y organizaciones ágiles. Arandu Utic, 6(1), 15–50.

Wang, Y., & Nor, E. (2022). The impact of fintech on the profitability of traditional banks. Global Business & Management Research, 14.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. Artificial Intelligence Review, 1– 25.

Zhou, H., Shen, T., Liu, X., Zhang, Y., Guo, P., & Zhang, J. (2020). Survey of knowledge graph approaches and applications. Journal on Artificial Intelligence, 2(2), 89–101.