AI & Cybersecurity – connection, impacts, way ahead

Oana-Alexandra SARCEA (MANEA),
SNSPA University, Bucharest, Romania
oana.manea89@gmail.com

Abstract

Artificial intelligence (AI) and cybersecurity have a strong connection and impact each other in different ways. An overview is related to the following categories: detection and prevention, automated response, adversarial AI, data protection, risk assessment, privacy concerns. Looking ahead, the linkage between AI and cybersecurity will continue to evolve. Key areas of focus include: development of AI-driven security solutions, ethical AI-use, enhanced threat intelligence, human-machine collaboration. Overall, AI holds tremendous potential to revolutionize cybersecurity, but it also presents new challenges that must be addressed to ensure a secure and resilient digital environment. The relationship between AI and cybersecurity is multifaceted. AI technologies are increasingly being employed both to enhance cybersecurity defenses and to facilitate cyberattacks. In addition to the above key points, is to mention the cybersecurity skills gap: with the growing complexity of cyber threats, there is a shortage of skilled cybersecurity professionals. AI technologies can help bridge this gap by automating routine tasks and augmenting the capabilities of existing security teams. Behavioral analysis is another important element: AI-powered systems can analyze user and network behavior to identify anomalies that may indicate a security breach. By understanding typical behavior, AI can detect deviations that might signal an attack. Overall, the relationship between AI and cybersecurity is complex and evolving. While AI offers significant opportunities to enhance cybersecurity defenses, it also presents new challenges and risks that must be addressed. Ongoing research and development are essential to stay ahead of emerging threats in this rapidly evolving landscape.

Keywords: new technologies, AI benefits, cybersecurity challenges, AI-cybersecurity linkage.

1. Introduction

Digitalization has a big impact on all parts of a business and can alter fundamentally the way how an enterprise provides value and operates with its consumers [1]. Digital systems should be designed for peaceful use, but their potential for both beneficial and harmful applications has been explored extensively in the cybersecurity literature [2, 3]. One effective response to cyberattacks can be artificial intelligence (AI), which can automate threat detection and mitigation, ensuring a rapid and accurate response to various types of attacks. AI can analyze behavioral patterns and unusual activities in real-time, thereby identifying subtle indicators of attacks. Moreover, it can continuously adapt defense strategies based on automated learning from previous incidents. By incorporating AI within cybersecurity teams, organizations can gain an edge in combating cyber threats in an ever-changing and increasingly sophisticated environment. Artificial intelligence (AI) stands as a potent technology empowering cybersecurity teams to automate repetitive tasks, expedite threat detection and response, and enhance the precision of actions, thereby fortifying security against a spectrum of threats and cyberattacks. These undertakings align with the seamless integration of AI-based cybersecurity in today's landscape of digital transformation and multifaceted challenges [4].

Artificial intelligence and machine learning technologies play pivotal roles in this dynamic defense landscape, enabling organizations to detect anomalies, predict potential threats, and respond swiftly to emerging cyber risks.

AI is already a key technology in our economy, poised to bring transformative changes similar to those brought by the steam engine or electricity. However, concerns about potential loss of control in the human-AI relationship are increasing [5]. Issues such as autonomous driving and the opaque decision-making processes of vehicles, particularly in extreme situations just before a collision, have long been topics of public debate. Similar concerns arise regarding the extent to which AI should support or even make medical decisions independently. It will often be crucial to understand how a machine's decision was made and to evaluate the quality of its explanation [6].

In the age of digital interconnectivity, managing security vulnerabilities has become increasingly complex. Organizations face a growing number of potential vulnerabilities and often struggle to manage them effectively. Traditional vulnerability management approaches, which are typically reactive and address high-risk vulnerabilities only after they have been exploited [7], are inadequate in today's cybersecurity environment.

In this context, Artificial Intelligence plays a transformative role in vulnerability management. The combination of AI and Machine Learning (ML) offers a proactive and predictive approach. One significant method is User and Event Behavioral Analytics (UEBA), which enables AI systems to continuously analyze and learn from the baseline activities of an organization's user accounts, endpoints, and servers. This ongoing analysis helps identify abnormal behaviors that deviate from the established norms, potentially indicating zero-day attacks. Zero-day attacks exploit unknown vulnerabilities before developers can create and distribute patches, making them particularly dangerous [8]. AI and UEBA can detect these attacks much earlier in their lifecycle.

2. Artificial Intelligence and Cybersecurity connection

In an era marked by increasingly harmful and frequent cyberattacks, artificial intelligence (AI) adds an extra layer of complexity to an already entropic environment, for worse or better. While the recent debate revolves mostly around the challenges and security concerns posed by AI, the technology also provides the cybersecurity sector innovative ways to defend against hostile different actors. As a result, the market for AI in cybersecurity is expected to show considerable growth in the coming years, from around 24 billion U.S. dollars in 2023, to roughly 134 billion U.S. dollars by 2030.

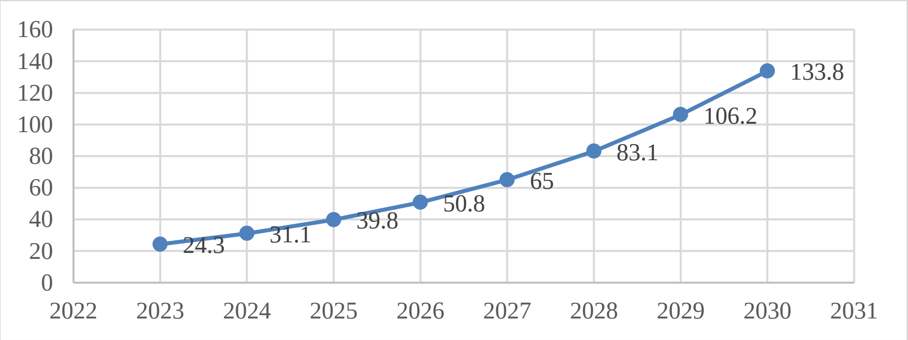


Fig. 1. Value of Artificial Intelligence (AI) and cybersecurity market worldwide from 2023 to 2030 (in billion U.S. dollars)
Source: Author's representation after A. Borgeaud, 18.03.2024, Statista
https://www.statista.com/statistics/1450963/global-ai-cybersecurity-market-size/

Many of the technologies influencing digital transformation are not novel innovations. The innovation lies in the integration of information, computing, communication, and connectivity technologies. The key technological domains enabling digital transformation are diverse and are commonly referred to as "general-purpose technologies" [9]. These encompass cyber-physical systems (CPS), the industrial internet of things (IoT), cloud computing (CC), big data (BD), artificial intelligence, and even augmented and virtual reality [10].

The significant impact of digital transformation on firms' processes and capabilities, as well as the alterations these technologies drive within industrial and organizational activities, has gained increasing academic attention in recent times. Digital transformation encompass a wide array of technological advancements, including the Internet of Things (IoT), Additive Manufacturing, Big Data, Artificial Intelligence, Cloud Computing, Augmented and Virtual Reality, and Blockchain, among others [11].

Fig. 2. Representations from craiyon.com after "Artificial Intelligence and Cybersecurity connection"

As companies traverse the path of digital metamorphosis, the very fabric of their operations undergoes a profound shift. This shift is characterized by the integration of cutting-edge technologies such as artificial intelligence, cloud computing, and the Internet of Things into daily business processes. The digital era heralds unparalleled opportunities for efficiency gains, enhanced customer experiences, and unprecedented innovation. However, this transformative journey is not without its perils.

The integration of artificial intelligence and machine learning in cybersecurity is a burgeoning area of research, as scholars explore how these technologies can enhance threat detection and response capabilities [12].

The integration of artificial intelligence and machine learning into business processes is a significant aspect of digital transformation. These technologies enable organizations to extract valuable insights from vast amounts of data, automate decision-making processes, and enhance the overall efficiency of operations. Predictive analytics powered by machine learning algorithms, for example, can help organizations forecast trends, identify potential risks, and make informed decisions.

In the realm of human resources, automation transforms traditional hiring processes. Intelligent recruitment tools, powered by artificial intelligence (AI), analyze resumes, assess candidate suitability, and even conduct initial interviews. This not only accelerates the hiring cycle but also ensures a more data-driven and objective selection process, contributing to the acquisition of top-tier talent.

Technology, particularly data analytics and artificial intelligence, serves as the enabler of personalization. By leveraging customer data, businesses can unveil patterns, predict preferences, and tailor offerings to suit individual tastes. Recommendation engines, fueled by algorithms that discern purchase histories and browsing behaviors, elevate the customer experience by presenting relevant and personalized content [13].

Parallel to the cloud revolution is the integration of data analytics and artificial intelligence, reshaping how organizations derive insights, make decisions, and create value. The vast volumes of data generated in the digital age hold immense potential, but unlocking that potential requires advanced analytical tools and intelligent systems [14].

3. Methodology and impacts

3.1. Technical manner and explanations for the used VOSviewer method

Scopus (TITLE-ABS-KEY ("artificial intelligence") AND TITLE-ABS-KEY ("Cybersecurity")).

Subject area: Business, Management and Accounting: 197; Economics, Econometrics and Finance: 98; Total items: 224.

Web of science -> selected only business economics for research areas -> result 54 items. “artificial intelligence” (Topic) and cybersecurity (Topic); Manually merged duplicates in Zotero -> Result: 238 items; Type of analysis: Co-occurrence; Unit of analysis: keywords; Counting method: full counting.

Table 1. Thesaurus file

Label	**Replace by**
cyber security	cybersecurity
artificial intelligence (ai)	artificial intelligence
ai	artificial intelligence
machine-learning	machine learning
internet of things (iot)	internet of things
iot	internet of things
block-chain	blockchain
cyber-attacks	cyber threats
data privacy	data protection
data security	data protection
risk assessment	risk mitigation
risk management	risk mitigation
digitalization	digital transformation
intrusion detection	intrusion detection system

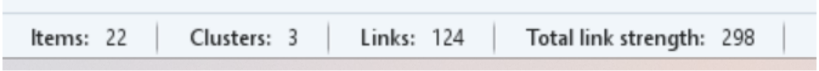
deep learning	machine learning
learning systems	machine learning
learning algorithms	machine learning

Minimum number of occurrences: 6; of the 1446 keywords, 27 meet the threshold.

Table 2.

Keyword	Occurrences	Total Link Strength
Cybersecurity	112	342
Artificial Intelligence	119	329
Machine Learning	52	159
Network Security	24	112
Internet of Things	27	103
Blockchain	22	88
Cyber Threats	19	69
Intrusion Detection System	15	58
Computer Crime	12	55
Digital Transformation	19	55
Risk Mitigation	12	47
Information Management	8	37
Security	11	37
Data Protection	13	35
Decision Making	8	32
Big Data	8	31
Sustainable Development	6	31
Denial-of-Service Attack	6	30
Sustainability	7	29
Crime	7	28
Automation	7	25
Malware	6	25
Behavioral Research	7	23
Industry 4.0	12	22
Security of Data	8	21
Fintech	8	16

Excluded elements: cybersecurity, artificial intelligence (search terms); security, crime, ‘current (general terms):



Items: 22 | Clusters: 3 | Links: 124 | Total link strength: 298

Fig. 3.

The network consists of 22 items, organized into a focused set of keywords. These keywords are grouped into 3 distinct clusters, indicating that the topics covered fall into three main thematic areas. There are 124 links, suggesting numerous connections between these keywords, creating a rich web of relationships and co-occurrences. The total link strength of 298 further emphasizes the robustness of these connections, indicating that the keywords frequently appear together in the literature, reflecting strong thematic interdependencies.

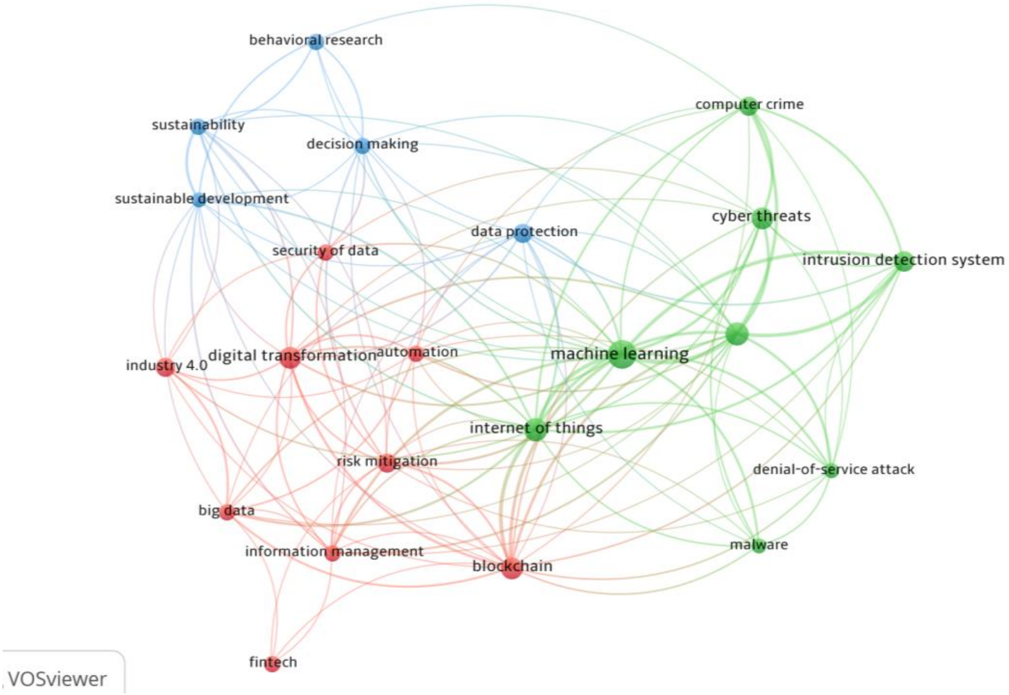


Fig. 4. VOSviewer Artificial Intelligence and Cybersecurity keywords (after technical and rationale methods applied)

Table 3.

Cluster	Keywords
Red Cluster	automation, big data, blockchain, digital transformation, fintech, industry 4.0, information management, risk mitigation, security of data
Green Cluster	computer crime, cyber threats, denial-of-service attack, internet of things, intrusion detection system, machine learning, malware, network security
Blue Cluster	behavioral research, data protection, decision making, sustainability, sustainable development

The red cluster emphasizes the transformative power of technology in industries, particularly fintech, and Industry 4.0. Fintech is reshaping financial services with innovations like blockchain, which ensures secure and transparent transactions. Automation and big data analytics are revolutionizing how financial institutions operate, making processes faster and more efficient. Industry 4.0 incorporates sophisticated technologies like the IoT and robotics into manufacturing, creating smarter factories where machines optimize production through communication. Digital transformation in these sectors involves more than just adopting new technologies; it also requires changing business models and processes to remain competitive. Managing information effectively and mitigating risks is crucial in this tech-driven landscape, ensuring that data security remains a top priority.

The green cluster focuses on cybersecurity, emphasizing how machine learning and artificial intelligence (AI) enhance security systems. Machine learning algorithms are able to verify extensive amounts of data to find distinctive patterns and potential threats in real time. For instance, AI-powered intrusion detection systems can identify and respond to cyber-attacks faster than traditional methods. These technologies learn from past incidents to improve their accuracy, making it harder for malicious activities to go unnoticed. The IoT is expanding the attack surface, making robust cybersecurity measures even more critical. By leveraging AI and machine learning, cybersecurity systems become more adaptive and proactive, effectively safeguarding against evolving cyber threats such as malware, denial-of-service attacks, and other forms of computer crime.

The blue cluster, delves into sustainability, decision-making, and data protection, presenting a holistic approach to modern challenges. Behavioral research in this cluster examines how people's actions and decisions impact sustainability efforts and data security. Understanding these behaviors helps in designing better policies and practices that promote sustainable development. Data protection is another critical aspect, ensuring that personal and sensitive information is secure from breaches. This cluster also emphasizes the importance of informed decision-making in achieving sustainability goals. Decision-making processes need to be grounded in reliable data and consider long-term environmental, social, and economic impacts. By integrating sustainability into every decision, from policy-making to daily operations, organizations can contribute to a more sustainable future. This approach balances immediate needs with the well-being of future generations, ensuring that development is both responsible and resilient.

The infusion of emerging technologies such as artificial intelligence (AI) and machine learning (ML) facilitates the creation of intelligent systems capable of learning, adapting, and making informed decisions autonomously. This not only augments operational efficiency but also empowers businesses to glean actionable insights from vast troves of data, steering them towards more informed and strategic decision-making.

The integration of artificial intelligence (AI) into communication systems enhances efficiency and personalization. AI-powered chatbots, for instance, facilitate instant responses to routine queries, freeing up human resources to focus on more complex tasks. Machine learning algorithms analyze communication patterns, providing insights into team dynamicArtificial intelligence (AI) injects a layer of sophistication into communication systems. AI-driven chatbots, for instance, offer instantaneous responses to routine queries, enhancing the efficiency of information retrieval. Machine learning algorithms sift through communication patterns, unveiling valuable insights into team dynamics and areas where communication can be refined. The synergy between human intuition and AI precision augments the efficacy of communication processess and identifying areas for improvement in collaboration and workflow [15].

AI-powered platforms, and networks that generate vast amounts of data. Network Security is a critical element and a subfield of cybersecurity and is closely linked to it. The Internet of Things (IoT) is also deeply tied with both digital transformation and cybersecurity, indicating the rapid development and growing concerns related to security challenges presented by IoT devices. Artificial Intelligence (AI) has been a highly researched area in recent years and has the potential to disrupt business practices by enhancing capabilities in technology systems. Its role is becoming increasingly important in the digital economy and in IT practices within the field of cybersecurity.

Artificial intelligence and machine learning technologies play pivotal roles in this dynamic defense landscape, enabling organizations to detect anomalies, predict potential threats, and respond swiftly to emerging cyber risks.

As organizations migrate their operations to cloud environments, the paradigm of cybersecurity undergoes a fundamental shift. Cloud computing introduces a new dimension of flexibility and scalability, allowing companies to scale resources on-demand. However, this flexibility also raises concerns about data sovereignty, regulatory compliance, and the security of shared cloud infrastructure. Cybersecurity strategies must align with the nuances of cloud environments, encompassing robust identity and access management, encryption protocols, and continuous monitoring to ensure the integrity of data stored in the cloud [16].

The human element in cybersecurity remains a critical factor that cannot be overlooked. Employees, often unwittingly, become vectors for cyber threats through social engineering, phishing attacks, or unintentional data breaches. Establishing a culture of cybersecurity awareness becomes imperative. Companies must invest in comprehensive training programs, educating employees about the evolving tactics of cyber adversaries and instilling a sense of responsibility for safeguarding sensitive information.

3.2. Way ahead

Artificial intelligence needs rich and accurate knowledge, just like authentic human experiences. At the same time, they must have a deep understanding of users, including their psychographic characteristics. [17].

I refers to the ability of a machine or computer to mimic the capacities of the human mind, which often learns from past experiences to respond and understand the language, complex problems and decisions. When incorporated into cybersecurity operations, AI is expected to improve vulnerability management and threat detection and accelerate incident response times. More than this, AI could also contribute to easing talent shortage issues in cybersecurity operations. Overall, improved security constituted the main benefit of AI initiatives in enterprises in 2023. Nevertheless, the integration of AI into cybersecurity processes is not without risks as AI, particularly generative AI, can be used to advance adversarial capabilities, such as malware development, phishing and deepfakes [18].

AI is gaining attention in most quadrants of economy and the society, as it can plays a key role in the ongoing digital transformation and impact people's daily lives through its automated decision-making capacities. AI is also seen as an important enabler of cybersecurity innovation for two main reasons: its ability to respond and detect the cyber threats and the need to secure AI-based applications.

4. Conclusion

As a conclusion, artificial intelligence significantly enhances cybersecurity capabilities through automation, predictive analytics, advanced threat detection and adaptive learning. It also introduces new challenges and demands ongoing management to ensure ethical use and effectiveness. AI has become a driving force for cyber threats, enabling adversaries to launch more effective and sophisticated attacks at a larger scale and faster. Cybersecurity has evolved along with information and technology systems to become an important aspect of the contemporary world; the development of artificial intelligence opens up new ideas for overcoming cybersecurity difficulties [19]. The field of cybersecurity has been very much impacted by artificial intelligence. It is an essential tool for information protection due to its identification' capacity, evaluate, and avoid cyber risks. Artificial intelligence can scan huge volumes of data, anticipate weaknesses and spot anomalies, assisting companies and people in more effectively and quickly defending against attacks. Successful applications of AI in cybersecurity already present the technology's advantages and promise. To overcome opposition in a successful manner and reach a high degree of cybersecurity maturity, it is decisive to be advanced in technology continuously and have abilities and knowledge in this area.

References

[1] B. Hinings, T. Gegenhuber and R. Greenwood, "Digital innovation and transformation: An institutional perspective," *Information and organization,* 2018 March 2018.

[2] J. Nye, "How Will New Cybersecurity Norms Develop?," *Strategist*, 12 March 2018.

[3] T. Riebe and C. Reuter, "Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment," 2019. [Online]. Available: https://link.springer.com/content/pdf/10.1007/978-3-658-25652-4_8.pdf.

[4] R. Kaur, D. Gabrijelčič and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," 2023.

[5] A. Holzinger, G. Langs, K. Zatloukal and H. Müller, "Causability and explainability of artificial intelligence in medicine," *WIREs Data Mining and Knowledge Discovery,* vol. 9, no. 4, 2019.

[6] R. R. Hoffman, S. T. Mueller, G. Klein and J. Litman, "Metrics for explainable AI: Challenges and prospects," Cornell University, 2018.

[7] S. Kumar, U. Gupta and A. K. Singh, "Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era," *Journal of Computers, Mechanical and Management,* vol. 2, no. 3, pp. 31-42, 2023.

[8] K. Al-Dosari, N. Fetais and M. Kucukvar, "Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges," *Cybernetics and Systems,* 2022.

[9] H. Hirsch-Kreinsen and M. T. Hompel, "Digitalisierung industrieller Arbeit: Entwicklungsperspektiven und Gestaltungsansätze," 2017.

[10] X. Cheng, J. Sun and A. Zarifis, "Artificial intelligence and deep learning in educational technology research and practice," *British Journal of Educational Technology,* 2020.

[11] A. Rindfleisch, M. O'Hern and V. Sachdev, "The Digital Revolution, 3D Printing, and Innovation as Data," *J PROD INNOV MANAG,* 2017.

[12] M. Ettredge, F. Guo and Y. Li, "Trade Secrets and Cybersecurity Breaches," *Journal of Accounting and Public Policy,* vol. 37, no. 6, 2018.

[13] A. Kuzior, P. Brożek, O. Kuzmenko, H. Yarovenko and T. Vasilyeva, "Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends," *Journal of Risk and Financial Management,* 2022.

[14] D. Teece, "Business models and dynamic capabilities," *Long Range Planning,* 2018.

[15] M. Malatji and A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI," *AI Ethics,* 2024.

[16] D. Rammanohar and S. Raghav, "Artificial Intelligence in Cyber Security," *Journal of Physics: Conference Series,* 2021.

[17] C. Vrabie, "De la idee la implementare," *Traseul sinuos al inteligentei artificiale catre maturitate,* vol. 1, 2024.

[18] A. Borgeaud, "Artificial intelligence (AI) in cybersecurity - statistics & facts," [Online]. Available: https://www.statista.com/topics/12001/artificial-intelligence-ai-in-cybersecurity/#topicOverview.

[19] R. Fazley, "Artificial Intelligence in Cyber Security," *SSRN,* 2024.