CogNexus *Volume: 1 Issue:2 04/2025/pp. 26- 36*

A Multidisciplinary, Multilingual, International, Peer-Reviewed, Open Access Journal

THE INTERSECTION OF ARTIFICIAL INTELLIGENCE AND HUMAN DECISION-MAKING IN CYBERSECURITY RESILIENCE: BUSINESS ANALYSIS PERSPECTIVE

[1] Blessing Unwana Umoh
[2] Alliy Adewale Bello
[3]Nonso Okika
[4]Chioma Emmanuela Ukatu
[5]Agboola Olatoye Kabiru

[1]Department of Business Administration & Management of Information Systems, University of Pittsburgh
[2]College of Professional Studies, Roux Institute, Northeastern University
[3]Network Security Analyst, University of Michigan
[4]Business Analyst, Sony Interactive Entertainment, U.S.A
[5]Department of Business Analytics & Data Science, New Jersey City University

Abstract

This review investigated the complex interplay of Artificial Intelligence (AI) with human decisions in building cybersecurity resilience from a business analysis viewpoint. It investigated how AI can optimize human decision-making, escalate security measures, and guarantee swift action in response to any form of cyberattack while factoring in the contribution of human judgment, intuition, and oversight into consideration for intense decisions. This review further investigated the impact of AI automation on information technology security risks in conjunction with human strategic management, focusing on their collective role in enhancing and sustaining cybersecurity resilience in organizations and across sectors. Existing credible journals and materials formed the datasets utilised for this review. Findings from examined journals and materials were presented thematically. Key findings revealed that the role of human decision-making in building AI cybersecurity resilience is critical. Stakeholders in AI cybersecurity need to properly integrate human factors to build concrete resilience against various cyberattacks.

Keywords: Artificial Intelligence, Human, Decision making, Cybersecurity resilience, Business Analysis

Résumé

Cette revue a examiné l'interaction complexe entre l'intelligence artificielle (IA) et les décisions humaines dans la construction de la résilience en cybersécurité, dans une perspective d'analyse commerciale. Elle a exploré comment l'IA peut optimiser la prise de décision humaine, renforcer les mesures de sécurité, et garantir une réponse rapide à toute forme de cyberattaque, tout en tenant compte du jugement, de l'intuition et de la supervision humaine dans les décisions critiques. Cette étude a également analysé l'impact de l'automatisation par l'IA sur les risques liés à la sécurité des technologies de l'information, en lien avec la gestion stratégique humaine, en mettant l'accent sur leur rôle conjoint dans le renforcement et le maintien de la résilience en cybersécurité au sein des organisations et à travers différents secteurs. Des revues et

documents crédibles existants ont constitué les bases de données utilisées pour cette analyse. Les résultats issus des documents examinés ont été présentés de manière thématique. Les principales conclusions révèlent que le rôle de la prise de décision humaine dans la construction d'une résilience en cybersécurité par l'IA est essentiel. Les parties prenantes dans le domaine de la cybersécurité assistée par l'IA doivent intégrer de manière adéquate les facteurs humains pour bâtir une résilience solide face aux diverses cyberattaques.

Mots-clés : Intelligence artificielle, Humain, Prise de décision, Résilience en cybersécurité, Analyse commerciale

1. Introduction

1.1 Artificial Intelligence (AI) and Cybersecurity

The emerging integration of Artificial Intelligence (AI) into cybersecurity in recent times is critical. The advantages of AI manifested in real-time analysis, machine learning, and predictive analytics cannot be overemphasized (Hoffman, 2021; Bécue et al., 2021). The contributions of AI to cybersecurity cannot be ignored. The real-time analysis of large volumes of data enables powered threat detection systems to spot patterns that suggest malicious activity. Organizations enhance their ability to detect and manage security incidents through machine learning algorithms that adapt to new cyber threats by learning from historical data. Organizations benefit from AI security platforms as they automate incident response operations, which enable rapid mitigation of security incidents across large networks. Organizations can optimize their incident response operations and minimize detection and remediation time for security incidents through the combination of AI technologies with existing security tools and processes (Hoffman, 2021). AI algorithms analyze past security information to discover trends and predict upcoming cyber-attacks while guiding organizations to allocate resources and investments in security wisely. Predictive analytics helps organizations take early action against new cyber threats and improve resource distribution to reduce security risks. The use of adversarial training techniques and robustness testing helps AI systems become more resistant to adversarial attacks. Organizations that integrate adversarial examples in their AI training procedure enhance model robustness and minimize their vulnerability to unauthorized manipulation. AI technologies process large volumes of threat intelligence from multiple sources to detect new cyber threats and enable proactive defence mechanisms. Organizations can gain deeper insights into adversary TTPs through correlation and contextual analysis of threat intelligence feeds, which enables them to develop effective countermeasures (Hoffman, 2021; Bécue et al., 2021).

In cybersecurity, AI has moved to the front of the line, and now there is a better, faster way to find, prioritize, evaluate, and respond to these dangers than at any other point in time (Chowdhry et al., 2020). Traditional cybersecurity platforms are based on preconfigured rules and signature-based methods of attack detection, which are proving to be inept with the rising new or unprecedented attacks. However, unlike AI-driven systems and machine learning algorithms, they can pick up patterns of malicious behavior even without any known signature (Arakpogun et al., 2021). Moreover, AI is also useful in determining the level of contribution of cybersecurity threats and the probability of such threats. By studying data involved in past occurrences, vulnerabilities, and the greater threat realm of a vulnerability, AI can prioritize risks for their probability and their impact. The capability of prioritization allows organizations to choose higher risks while having baseline controls for lesser priorities (Maddireddy & Maddireddy, 2021). Mitigation is yet another field in which AI is making a revolution. AI may be employed for automating typical cybersecurity activities such as patch application, quarantining compromised systems, IP blocking, decreasing response times, and minimizing human intervention. For instance, AI-driven endpoint security technologies can quarantine machines with suspicious activity and prevent malware propagation within the network of an organization. This future-oriented approach is in addition to an organization's overall security position and reduces downtime caused by security incidents (Ganesh & Kalpana, 2022).

1.2 Automation in Detecting Anomalies and Responding to Breaches

One of the most notable contributions of AI to cybersecurity is automation, which is especially evident in anomaly detection and breach response. It is no longer possible to monitor everything manually in contemporary networks, which have an incredible amount of data and infrastructure intricacy. Automated systems are capable of constantly evaluating streams of data, detecting divergences from standard patterns, and sending warnings when threats might be present (Shah, 2021). AI-based anomaly detection utilizes ML algorithms to develop system, application, and user baseline behavior. For instance, the system can flag this behavior as suspicious if an employee accesses a large number of sensitive documents outside of regular working hours or from an unusual location. This real-time detection enables organizations to intervene early, potentially preventing breaches before they escalate into major problems (Jimmy, 2021). Besides detection, AI also greatly improves response capacity using Security Orchestration, Automation, and Response (SOAR) systems. AI-powered SOAR systems exploit AI to automate security incident analysis and remediation. For instance, in the case of a phishing attack, an AI-based SOAR system can process malicious emails, detect impacted users, and automatically quarantine compromised accounts while notifying the security team. This degree of automation quickens the speed of response and alleviates the burden on human analysts so that they can dedicate their time to more sophisticated threats (Kinyua & Awuah, 2021). AI also plays a key role in post-incident handling and recovery. In case of a breach, AI systems can process forensic information to decide on the attack vector, detect the affected assets, and recommend remediation processes. This realization is invaluable in future attack prevention and in strengthening the cybersecurity defense of the organization (Bernadette et al., 2022).

Though AI has immense potential to improve threat detection and response, it also entails risks regarding data security, trust, ethics, and adversarial AI (Banik & Dandyala, 2023). A complex strategy comprising strong defenses against adversarial attacks, strict data protection mechanisms, improved transparency in AI decision-making, and clear ethical guidelines is necessary to mitigate these risks. Through the successful navigation of these hurdles, businesses can leverage AI's capabilities to augment cybersecurity operations while maintaining ethical and regulatory concerns in view (Bonfanti, 2022).
Essentially, the role of human decision-making in cybersecurity resilience needs to be examined and evaluated. In addition, the interplay between AI and human decision-making can play a critical role in advancing cybersecurity resilience.

2. Literature Review

2.1 Role and Challenges of AI in Cybersecurity

The increased integration of AI into cybersecurity mechanisms has various advantages, including improved threat detection, automated incident response, and predictive analytics. In general, despite these enormous benefits, there are tremendous challenges accompanying them to ensure they can be deployed effectively and ethically in the domain of cybersecurity. One of the most critical issues in the domain of AI in cybersecurity is the emergence of malicious AI (Egbuna, 2021). Today, AI techniques are being employed by cyber attackers to develop new and evasive attacks that existing security mechanisms cannot stop. The act of tricking a machine learning algorithm is known as adversarial AI, and it consists of feeding the machine learning algorithms misleading input that is going to produce an erroneous output. This kind of technique can be used in many ways, for example, bypassing intrusion detection systems or fake phishing emails to bypass spam filters. For example, they can attack by manipulating malware to make it appear benign to security systems that are powered by AI. Thus, if the cybersecurity experts lose, AI will be grounded and unable to detect and destroy threats, resulting in an arms race between the cybersecurity experts and the attackers. The rise in the adversarial attacks associated with AI systems raises the need for defensive measures to guard against adversarial attacks (Aldahdooh et al., 2022). Also, some of these attacks can be automated and scaled by attackers, so they could produce more attacks that may exceed current security configurations in volume. Continuous upgrading and adaptation of AI models are necessary to fight against new threats.

Furthermore, when AI is integrated into cybersecurity, there is data privacy, which is of utmost importance to gather and process huge volumes of data. To train the AI software models effectively, AI software needs

to see confidential information, including PII, financial data, and other confidential data (Dash et al., 2022). However, both breaching or misuse of such data could represent a great danger to the protection of individuals' privacy rights (Citron & Solove, 2022). Secondly, AI algorithms can unintentionally lead to biased decision-making. For example, an AI system trained using biased data can have a disproportionate number of certain individuals or groups flagged as potential threats based on defective assumptions. This bias can result in serious consequences, for instance, wrongful incrimination or exclusion of certain groups from essential services. Reducing these issues of privacy entails the implementation of strict data protection measures, for example, anonymization, encryption, and strong data access controls (Thapa & Camtepe, 2021). Additionally, organizations need to ensure adherence to privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) that prescribe strict guidelines on personal data collection and processing. Transparency and trust in AI decision-making are crucial to the success of AI integration into cybersecurity (Hamon et al., 2022). The majority of organizations find it difficult to explain how AI models arrive at specific conclusions or suggestions, and that makes stakeholders and users distrust them. Lack of explainability can hinder the uptake of AI technologies because individuals may not be ready to trust systems that are poorly understood. Furthermore, the "black box" nature of the majority of AI algorithms, particularly deep learning models, renders it challenging to ascertain their reliability and performance (Tschider, 2020). The users will be unable to comprehend the way that the models arrive at their decisions, hence lacking trust in their output. This is a significant issue in the field of cybersecurity, given that decision-making affects considerably organizational security. To build trust in AI-driven cybersecurity systems, organizations need to focus on transparency so that it is evident how AI models function and how they are driven to make decisions. Additionally, applying explainable AI (XAI) techniques can demystify AI processes so that stakeholders understand and determine the trustworthiness of AI outputs (Langer et al., 2021).

Ethical issues of AI in cybersecurity are another significant challenge. The application of AI technologies may also raise ethical issues related to surveillance, consent, and the possibility of abuse (Fontes et al., 2022). For example, AI may be utilized by organizations to monitor employee behaviour or analyze user data for security purposes, thereby raising privacy violations and ethical use of surveillance technologies issues. Moreover, the legal environment around AI applications in cybersecurity is still evolving. Regulators are grappling with how to regulate AI technologies in a manner that wards off potential harms while fostering innovation (Lescrauwaet et al., 2022). The lack of clear-cut regulations can leave organizations seeking to implement AI-powered solutions unclear on what they should comply with or how they could be liable. To surmount such ethical and regulatory challenges, organizations must take the initiative by formulating clear ethical frameworks for AI use in cybersecurity. Engaging stakeholders, including ethicists, attorneys, and affected communities, can help ensure AI applications are aligned with societal norms and promote responsible practices (Golbin et al., 2020). AI's integration with cybersecurity brings numerous advantages as much as challenges.

3. Methodology

This study employs a qualitative research design to explore the nexus of AI, human decision-making, and cybersecurity resilience. Secondary data collected from peer-reviewed articles, case studies, and industry reports were analyzed. Relevant literature published between 2017 and 2024 was collected using academic databases such as ResearchGate, Google Scholar, IEEE Xplore, and ScienceDirect. Keywords such as "AI in cybersecurity," "AI and human decision-making", “Cybersecurity resilience”, cybersecurity challenges", “AI and human factors”, and "AI-based cybersecurity", were used to search for relevant and credible journals and materials. Document analysis was employed, and results were presented thematically.

4. Results and Discussion

This section presents the results generated from the sourced and reviewed credible journals and materials on the integration of Human decision-making into AI cybersecurity resilience across sectors.

4.1 Case Studies: Successful Implementations of AI in Cybersecurity

Some cases have shown that AI is a transformative force of cybersecurity that works with many successful implementations. One particular example would be the instance of AI being used by Darktrace, one of the

world's leading cybersecurity companies using ML to discover and counteract cyberattacks. The platform provided by Darktrace is referred to as the Antigena and uses unsupervised machine learning algorithms to analyze network traffic patterns and derive indications from the patterns that someone might be attempting to exploit a network (Darktrace, 2023). With this approach, threats can be detected and responded to in real-time as a result, real-time threats and real-time responses can be automatic without human intervention, improving the privacy of data and integrity of information. Several high-profile organizations have seen that the company's implementation is successful, protecting all data, including the most sensitive, while keeping operations moving.

Another major instance is when Google uses AI in the course of its Project Shield initiative. To protect news websites and other high-value platforms from Distributed Denial of Service (DDoS) attacks, Project Shield uses Google's machine learning models. Using AI to analyze traffic patterns and detect the early warning of the attack, Google can provide strong protection against DDoS attacks, which may lead to website availability and integrity disorder (Google, 2023). The application of AI in that sense isn't only keeping the targeted sites secure but also keeping the information the sites have contents in and yet confidential. Also, the same IBM's Watson for Cyber Security is an exemplary use of AI to strengthen cybersecurity. Since Watson is looking at enormous amounts of data from several sources, security blogs, threat intelligence feeds, and internal security data, Watson uses natural language processing and machine learning so that it can analyse all this data. Through correlations, the types of threats and vulnerabilities can be pointed out, and Watson provides actionable insights that help an organization to be better at protecting their data and maintaining the integrity of their information (IBM, 2023). According to IBM, its solution has played a fundamental role in assisting organizations in tackling intricate cyber threats and protecting their digital environment.
However, in these cases, the role of human decision-making is not visible. The human factor role is essential in cybersecurity resilience,

4.2 Decision-Making in Cybersecurity

Security incidents are shaped by decision-making in the realm of cybersecurity. In cybersecurity, part of the effective decision-making comprises a risk assessment. This implies that they need to determine the threats, vulnerabilities, and potential impact of a cyberattack on the organization. By understanding these factors, resources can be devoted more efficiently, and security measures can be prioritized. This is also the point where the concept of risk aversion matters more than anything else because while the decision maker has to consider the costs of cybersecurity measures against the possible consequences of a breach, he certainly does. A critical decision for applying risk mitigation is balancing resource allocation and the risk mitigation itself, which is a complex, difficult-to-achieve decision by considering the risk landscape of an organization (Stevens, 2020). Knowledge and cyber awareness are critical assets in the making of cybersecurity decisions by a workforce. The first line of defense in cyber-attacks is the employees who know potential threats and best practices. For this reason, organizations implement cybersecurity awareness and training programs to ensure their staff can make decisions expected to happen under the cyber threat. From the IT department to every employee who works with digital systems, decision-making is no longer the limited role of IT but also business analysts, making education and awareness a key piece of the entire picture of a comprehensive cybersecurity strategy (Hummelholm, 2023).

Cybersecurity decision-making is not only inferred to the people but rather, the whole organization inclusive. The leadership and management teams have the responsibility for setting the tone for cybersecurity practices, making key decisions on the allocation of budgets, and developing policy and incident response strategies. These decisions have a high impact on an organization's ability to support cyber resilience. Such collaboration and communication are necessary to ensure that cybersecurity decisions align with the organization's higher-level goals (Hummelholm, 2023).

4.3 Collaborative Decision-Making

Decision-making in cybersecurity operations has been pointed out by literature on accountability, which should rest on humans (Verma et al., 2023; Lee et al., 2023). Jarrahi (2018) revealed that AI can help humans in the decision-making process by carrying out fast analysis of big data and sharing insights to operators with recommendations about the action they should take, and these insights would be completed

by human judgment that is consistent with the organizational values and strategies. The study further reiterated that true AI insights supplant human judgment with an accuracy beyond that of humans and do not usurp it by augmenting human judgment (Kapoor & Ghosal, 2022). Laux (2023) stressed that balanced decision-making and accountability necessitated that human oversight be present. Moreover, Bossaerts (2017) also inspired collaboration between automation, AI, and human expertise because it reaffirms AI's value as a supporting aid to decision-making. As Sitton and Reich (2018) stated, many scholars have called for an integrative framework for optimizing AI-human collaboration in decision processes.

4.4 Human Factors in AI-Enhanced Cybersecurity Resilience: Business Analysis Perspective

AI has now formed a new way of thinking about cybersecurity resilience. However, when AI is combined with cybersecurity, it is important not to forget the main role of human factors, especially as it relates to decision-making. AI-driven defense strategies continue to be a humanized solution influencing decision-making and implementation and in turn, overall effectiveness. The focus of this review is on the critical human factors in AI-enhanced cyber defense, its impact, challenges, and integration strategies (Alevizos and Dekker, 2024). However, AI's sophisticated ability to detect and respond to threats does and will rely on human expertise. During the democratization of data, cybersecurity professionals must receive domain knowledge, intuition, and contextual knowledge, which are necessary to understand the meaning of an AI-generated alert and decide intelligently. As an effective capability, AI can assist humans and ground their explanations, assess the severity of security incidents, and prioritize response actions more effectively by leveraging a desired range of business objectives and risk tolerance levels. Furthermore, human experts are involved in the fine-tuning of AI algorithms, detection rules refinement, and adaptation of a network defence strategy to counter existing cyber threats. Later down the line, when AI is fully integrated into cyber defence operations, you will need cybersecurity professionals whose background is in AI technologies. To be able to effectively deploy AI in use cases for defence, cybersecurity professionals need to be trained and skilled in the areas of AI. It also involves training on AI concepts, machine learning algorithms, and data analytics methods, as well as training on AI-powered security tools. Therefore, cybersecurity experts should remain updated on the new AI-driven threats and defense techniques (Whyte, 2020; Ronchi, 2022). For AI-enhanced cyber defence, effective collaboration and communication are very much crucial between human experts and AI systems. To make the best use of AI technologies, cybersecurity teams need to operate as one and coordinate different functional areas to drive response (Sontan & Samuel, 2024). Security incidents need some good incident response protocol and clear communication channels. Also, cybersecurity professionals, including business analysts, have to convey AI-generated insights and recommendations to non-technical people in an easy-to-understand and trustable way, which builds alignment across organizations and sectors (Sontan & Samuel, 2024; Marda, 2018).

Cybersecurity experts, including business analysts, at least to some degree, have a central role to play in terms of human factors in using AI in cyber defense ethically and responsibly. Given the guidelines of ethical standards, regulatory requirements, and organizational policies for the use of AI technology, cybersecurity professionals should follow the rules. This entails ensuring adherence to fairness, transparency, and accountability in the AI decision-making procedures, combating bias and discrimination, and respect for one's right to privacy (Dhabliya et al., 2023). In addition, cybersecurity professionals need to realize how AI in defense is also going to have wider societal ramifications, such as effects on the labor market, human rights, and societal well-being. Cognitive biases of humans can impact decision-making in AI-enhanced cyber defense, e.g., how or not to interpret results from AI-provided insights, as well as how or if implemented response actions are effective. Since confirmation bias, anchoring bias, and availability bias are among the cold fog of common cognitive biases, cybersecurity experts should identify themselves with them and take steps to reduce their impact. It may entail the use of decision support tools, conducting peer reviews, soliciting multiple perspectives to counter biased judgments as well as promoting more objective decision-making (Johnson, 2019; Dhabliya et al., 2023). Factors of user experience and usability of AI-powered security tools are critical for their adoption and effectiveness. From the point of view of human-centred cybersecurity, cybersecurity professionals need to evaluate the usability of AI-driven defense solutions on user interface design, workflow integration, and cognitive load. Their use makes cybersecurity professionals more instinctive and user-friendly to interact with AI systems, increasing their efficiency in the workflow and making their decisions more informed in highly stressful situations. Organizations should also seek feedback from end users who will be using these AI-powered security tools, as the feedback can

inform the design and development of the products. In the presence of rapidly evolving cyber threats as well as technological developments, a fundamental characteristic of AI in cyber defence that is of particular importance is human resilience and adaptability. Cybersecurity professionals need to be prepared to change course and adapt to the changes in AI-driven defence strategies as well as newer skills and techniques and adjust to new ways of attacking with the advancements in cybersecurity threats. A culture of resilience and adaptability within the cybersecurity teams builds innovation, creativity, and agility that make an organization a step ahead of what is evolving in terms of advances in cyber threats and retain its cyber defence capabilities.

Finally, human factors influence the use of AI to enhance cyber defense regarding decision-making, implementation, and overall effectiveness. To realize the power of using AI systems to defend against cyber threats, cybersecurity professionals such as business analysts must leverage their expertise, work with these systems to ensure cooperation at a high level, remain in line with ethical rules, reduce biases in cognition and remember, focus on the overall experience of the user, prepare for thriving and flexibility. Harnessing machine learning and AI technologies with human expertise can be leveraged by organizations to develop powerful and responsive cyber defences that span to stem evolving cyber threats to protect organizations and organization resources.

5. Conclusion

Achieving robust cybersecurity resilience requires the intersection of AI with human decision-making. Being able to detect threats, automate responses, and thus improve efficiency are all powers offered by AI. Nevertheless, ethical consideration, strategic alignment, and most importantly, creative problem-solving during a critical incident, hands down, though both human experts and AI play important roles. Business analysts have a crucial hand in steering this integration, keeping this integration in place that would see AI technologies supporting human decision-making instead of replacing it. By bringing forth the best of what AI possesses and the intelligence contribution of human factors, organizations can raise their cybersecurity resilience, outpace their cyber threats, and arm their digital assets. Review journals and materials recommended the development of a framework that will allow for the integration of human decision-making into AI cybersecurity resilience.

5.1 Future directions

As cybersecurity continues to evolve at the intersection of artificial intelligence (AI) and human decision-making, future research must embrace a transdisciplinary approach. To enhance cybersecurity resilience, it is essential to investigate beyond algorithmic efficiency and consider the socio-technical, communicative, pedagogical, and cultural contexts in which AI operates. A key area for further exploration is AI's communicative interface, particularly how it shapes and is shaped by human behavior and linguistic adaptation in digital spaces. Braimoh (2024) emphasizes that digital language, such as texting and symbolic shorthand, has profound implications for intercultural communication and pragmatic awareness. Applied to cybersecurity, this suggests that AI-human interaction models must adapt to emerging digital linguistic norms to improve usability and trust—critical factors in threat detection and user engagement. Additionally, strategic communication mechanisms are paramount in mitigating the ethical risks and societal impacts of AI technologies, particularly deepfakes. As Esezoobo and Braimoh (2023) argue, integrating legal and ethical education with communication strategies can help organizations and individuals navigate the threats posed by synthetic media. In cybersecurity contexts, such integration is vital for developing protocols that enhance transparency, legitimacy, and rapid response—particularly where AI-generated misinformation could trigger security breaches.

Building on the cultural and interpersonal dimensions of technological interaction, Onomejoh et al. (2024) provide valuable insights into how translation and interpersonal communication are used to navigate cultural sensitivity. AI applications in cybersecurity must similarly be culturally responsive. Systems must be trained not only on diverse data but also evaluated through culturally adaptive models to prevent algorithmic bias, especially in global cybersecurity environments where linguistic and cultural plurality is the norm. Another

future direction lies in the application of instructional design models to cybersecurity training. Omoregie, Anthony, and Braimoh (2025) stress the efficacy of models such as Addie, Sam, and Dick & Carey in designing adaptive online learning environments. These models can be repurposed to structure cybersecurity education and simulation-based training, tailoring them for asynchronous and blended contexts where professionals are trained to interact with AI tools effectively and ethically.

Moreover, e-learning platforms used for digital skill development during the Covid-19 pandemic, as discussed by Anthony, Braimoh, and Ehigie (2021), offer practical frameworks for scaling cybersecurity literacy. Their analysis of second language acquisition under infrastructural limitations parallels the need for inclusive cybersecurity awareness campaigns—especially in under-resourced regions where digital divides threaten resilience efforts. Future studies might explore how AI-driven cybersecurity tools can be localized linguistically and pedagogically for different communities. Finally, drawing from conflict resolution frameworks, Osekre et al. (2023) underscore the importance of communication and mediation in addressing psychological challenges. Similar principles can be applied to cybersecurity by designing human-AI interaction protocols that emphasize collaboration, mental health awareness (especially for frontline security analysts), and stress-reducing interfaces. Understanding how trust, mediation, and human emotion play into cybersecurity decision-making could redefine response strategies in high-stakes environments.
In summary, future research should adopt a holistic, human-centered, and interdisciplinary framework that accounts for strategic communication, digital language use, educational design, cultural sensitivity, and psychological resilience. Bridging these diverse areas will ensure that AI is not only technically robust but also ethically grounded, socially responsive, and adaptable to the dynamic needs of the cybersecurity landscape.

References

Aldahdooh, A., Hamidouche, W., Fezza, S. A., & Déforges, O. (2022). Adversarial example detection for DNN models: A review and experimental comparison. *Artificial Intelligence Review, 55*(6), 4403–4462.

Alevizos, L., & Dekker, M. (2024). Towards an AI-enhanced cyber threat intelligence processing pipeline. *arXiv preprint*, arXiv:2403.03265.

Anthony, H. M., Braimoh, J. J., & Ehigie, D. E. (2021). Challenges and adaptations in implementing e-learning for second language acquisition in Nigerian schools during the COVID-19 pandemic: A methodological analysis. *Journal of Emerging Technologies and Innovative Research, 8*(9), 407–419.

Arakpogun, E. O., Elsahn, Z., Olan, F., & Elsahn, F. (2021). Artificial intelligence in Africa: Challenges and opportunities. In *The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success* (pp. 375–388).

Banik, S., & Dandyala, S. S. M. (2023). The role of artificial intelligence in cybersecurity opportunities and threats. *International Journal of Advanced Engineering Technologies and Innovations, 1*(04), 420–440.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review, 54*(5), 3849–3886.

Bernadette, B.-A., Latifat, O. A., & Ogedengbe, D. E. (2022). Integrative HR approaches in mergers and acquisitions ensuring seamless organizational synergies. *Magna Scientia Advanced Research and Reviews, 6*(1), 078–085.

Bonfanti, M. E. (2022). Artificial intelligence and the offence-defence balance in cyber security. In *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation* (pp. 64–79). London: Routledge.

Bossaerts, P., & Murawski, C. (2017). Computational complexity and human decision-making. *Trends in Cognitive Sciences, 21*(12), 917–929.

Braimoh, J. J. (2024). Texting language as a digital symbolic current: Implications for pragmatics and intercultural communication in the digital age. *Journal of Studies in Language, Culture, and Society, 7*(2), 199–208.

Char, D. S., Abràmoff, M. D., & Feudtner, C. (2020). Identifying ethical considerations for machine learning healthcare applications. *The American Journal of Bioethics, 20*(11), 7–17.

Chowdhry, D. G., Verma, R., & Mathur, M. (2020). *The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security*. CRC Press.

Darktrace. (2022). *Darktrace AI: Combining Supervised and Unsupervised Machine Learning*. https://darktrace.com/resources/darktrace-ai-combining-supervised-and-unsupervised-machine

Dash, B., Sharma, P., & Ali, A. (2022). Federated learning for privacy-preserving: A review of PII data analysis in Fintech. *International Journal of Software Engineering & Applications (IJSEA), 13*(4).

Dhabliya, D., Gujar, S. N., Dhabliya, R., Chavan, G. T., Kalnawat, A., & Bendale, S. P. (2023). Temporal intelligence in AI-enhanced cyber forensics using time-based analysis for proactive threat detection. *Journal of Electrical Systems, 19*(3), 126–146.

Egbuna, O. P. (2021). The impact of AI on cybersecurity: Emerging threats and solutions. *Journal of Science & Technology, 2*(2), 43–67.

Esezoobo, S. O., & Braimoh, J. J. (2023). Integrating legal, ethical, and technological strategies to mitigate AI deepfake risks through strategic communication. *International Journal of Scientific Research and Management, 11*(08), 914–928. https://doi.org/10.18535/ijsrm/v11i08.ec02

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: Why we (might) need them and how we want them. *Technology in Society, 71*, 102137.

Ganesh, A. D., & Kalpana, P. (2022). Future of artificial intelligence and its influence on supply chain risk management–A systematic review. *Computers & Industrial Engineering, 169*, 108206.

Golbin, I., Rao, A. S., Hadjarian, A., & Krittman, D. (2020). Responsible AI: A primer for the legal community. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 2121–2126). IEEE.

Google. (2023). *Project Shield*. https://projectshield.withgoogle.com/

Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the gap between AI and explainability in the GDPR: Towards trustworthiness-by-design in automated decision-making. *IEEE Computational Intelligence Magazine, 17*(1), 72–85.

Hoffman, W. (2021). AI and the future of cyber competition. *CSET Issue Brief*, 1–35.

Hummelholm, A. (2023). AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks. *European Conference on Cyber Warfare and Security*.

IBM. (2023). *Watson for Cyber Security*. https://www.ibm.com/security/artificial-intelligence

Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human–AI symbiosis in organizational decision making. *Business Horizons*.

Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, 564–574.

Johnson, J. (2019). The AI–cyber nexus: Implications for military escalation, deterrence, and strategic stability. *Journal of Cyber Policy, 4*(3), 442–460.

Kapoor, R., & Ghosal, I. (2022). Will artificial intelligence compliment or supplement the human workforce in organizations? A shift to a collaborative human–machine environment. *International Journal on Recent Trends in Business and Tourism*.

Kinyua, J., & Awuah, L. (2021). AI/ML in security orchestration, automation and response: Future research directions. *Intelligent Automation & Soft Computing, 28*(2).

Langer, M., Oster, D., Speith, T., Hermanns, H., Kästner, L., Schmidt, E., Sesing, A., & Baum, K. (2021). What do we want from explainable artificial intelligence (XAI)? – A stakeholder perspective on XAI and a conceptual model guiding interdisciplinary XAI research. *Artificial Intelligence, 296*, 103473.

Laux, J. (2023). Institutionalised distrust and human oversight of artificial intelligence: Toward a democratic design of AI governance under the European Union AI Act. *SSRN Electronic Journal*.

Lee, H. W., Han, T. H., & Lee, T. (2023). Reference-based AI decision support for cybersecurity. *IEEE Access, 11*, 143324–143339.

Lescrauwaet, L., Wagner, H., Yoon, C., & Shukla, S. (2022). Adaptive legal frameworks and economic dynamics in emerging technologies: Navigating the intersection for responsible innovation. *Law and Economics, 16*(3), 202–220.

Maddireddy, B. R., & Maddireddy, B. R. (2021). Cybersecurity threat landscape: Predictive modelling using advanced AI algorithms. *Revista Española de Documentación Científica, 15*(4), 126–153.

Marda, V. (2018). Artificial intelligence policy in India: A framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), 20180087.

Omoregie, I., Anthony, H. M., & Braimoh, J. J. (2025). Comparative analysis of instructional models for designing effective online courses: ADDIE, SAM, and Dick & Carey approaches. *Journal of Languages & Translation, 5*(1), 33–45.

Onomejoh, P., Ehigie, D. E., Igbinovia, O., & Braimoh, J. J. (2024). Navigating cultural sensitivity in translation: The role of interpersonal communication in translating sensitive narratives. *Journal of Science and Knowledge Horizons, 4*(2), 204–229. https://doi.org/10.34118/jskp.v4i02.4020

Ronchi, A. M. (2022). Human factor, resilience, and cyber/hybrid influence. *Information & Security, 53*(2), 221–239.

Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Española de Documentación Científica, 15*(4), 42–66.

Sitton, M., & Reich, Y. (2018). EPIC framework for enterprise processes integrative collaboration. *Systems Engineering, 21*, 30–46.

Sontan, A. D., & Samuel, S. V. (2024). The intersection of artificial intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews, 21*(2), 1720–1736.

Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. *Digital War, 1*(1), 164–170.

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine, 129*, 104130.

Tschider, C. A. (2020). Beyond the "black box". *Denver Law Review, 98*, 683.

Umoh, B., Bello, A. A., Okika, N., Ukatu, C. E., & Kabiru, A. O. (2025). The intersection of artificial intelligence and human decision-making in cybersecurity resilience: Business analysis perspective. *CogNexus, 1*(2), 1–21.

Vaseashta, A. (2022). Nexus of advanced technology platforms for strengthening cyber-defense capabilities. In *Practical Applications of Advanced Technologies for Enhancing Security and Defense Capabilities: Perspectives and Challenges for the Western Balkans* (pp. 14–31). IOS Press.

Verma, R., Koul, S., & Ajaygopal, K. V. (2023). Evaluation and selection of a cybersecurity platform ─ Case of the power sector in India. *Decision Making: Applications in Management and Engineering*.

Whyte, C. (2020). Problems of poison: New paradigms and "agreed" competition in the era of AI-enabled cyber operations. In *2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 1300, pp. 215–232).