CogNexus: Volume: 1 Issue:1 1/2025/pp.(311-326)

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

Unmasking Vulnerabilities: AI-Powered Cybersecurity Threats and Their Impact on National Security

Exploring the Dual Role of AI in Modern Cybersecurity: A Threat and a Shield

[1]Joshua Seyi Ibitoye
jsibitoye@gmail.com
https://orcid.org/0009-0006-2355-5166

[2]Fatanmi Ebenezer Ayobami
Fatanmiayobami@gmail.com
https://orcid.org/0009-0004-1310-894X

[1]Southeast Missouri State University, USA.
[2]Nottingham Trent University, England.

Abstract

Artificial intelligence (AI) is redefining the cybersecurity world as a force for both a strong defense and an ever more sophisticated attack. This article critically examines AI with respect to the dual role it serves regarding recent breaches, AI's development as a tool for developing AI powered threats, and advancing AI powered defensive systems. Increasing reliance on AI driven tools by cybercriminals means high profile incidents like the Microsoft breach will continue. AI powered defense mechanisms, like behavioral analytics, predictive modeling, and automated response to incident, are increasing their utility as weapons against risks at the same time. AI is a dual use technology with ethical and practical challenges such as accessibility of malicious actors, accountability of implementation and widening gap between the resource rich and resource poor organizations. The article emphasizes the importance of doing global collaboration, additive AI on zero trust architecture and the regulations around responsible innovation. In this work, we provide a critical analysis on AI's abilities and the limitations it presents; highlighting the need to use AI responsibly and accordingly in the case of such risks embedded in the AI itself. To achieve it, governments, organizations and developers all need to work together to create adaptable systems that will navigate through continuously changing threat landscapes.

***Keywords*:** Artificial Intelligence, Cybersecurity, AI-Powered Cyberattacks, Predictive Threat Modeling, Automated Incident Response, Ethical AI Governance

Introduction: The Dual Role of AI in Cybersecurity

Artificial intelligence (AI) is moving at a rapid pace, opening up new opportunities and incredibly formidable dangers in the field of cybersecurity (Karthika et al., 2023). As cyber threats became increasingly evolved, AI is being utilized not only as a defensive but an offensive tool (Khan et al., 2024). Recent high profile cyber-attacks like Microsoft breach serve to underscore the way attackers are achieving higher level of sophistication of infiltrating systems with cloud vulnerabilities and leveraging AI driven tools (Mallick and Nath, 2024). According to IBM's Cost of a Data Breach Report (2023), the global cost of data breaches in 2023 alone already stood at an average of $5.17 million, up 2.25 percent from 2022. Additionally, compromised credentials were found to be the cause of 71% of these breaches, underlining the imperative of next generation AI defenses (IBM, 2024a). Figure 1 shows some of the most frequent AI-Powered Cyber-attacks

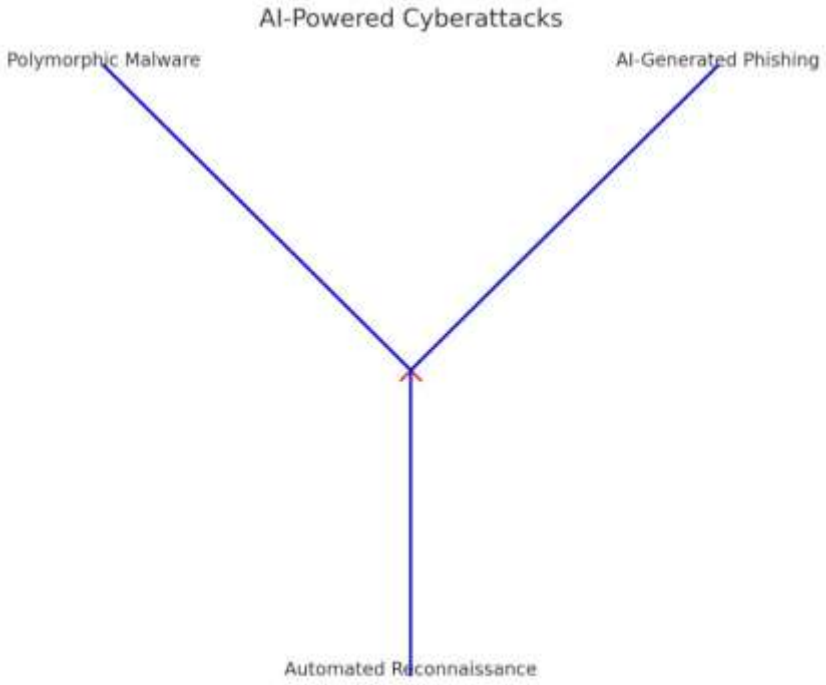

Figure 1: AI-Powered Cyber-attacks (Adopted from Aslan et al., 2023)

AI's transformative capabilities have also reshaped the defensive landscape as seen in Figure 2 (Obi et al., 2024). Organizations employing AI-based security measures can contain a breach faster, than with traditional methods (Secureframe, 2024). Meanwhile, the same technology is being used by attackers to run automated phishing campaigns, polymorphic malware, and more advanced reconnaissance efforts (Kumar et al., 2023). It is more urgent than ever, as cloud intrusions have increased on top of the defensive stance of businesses everywhere (World Economic Forum, 2024).

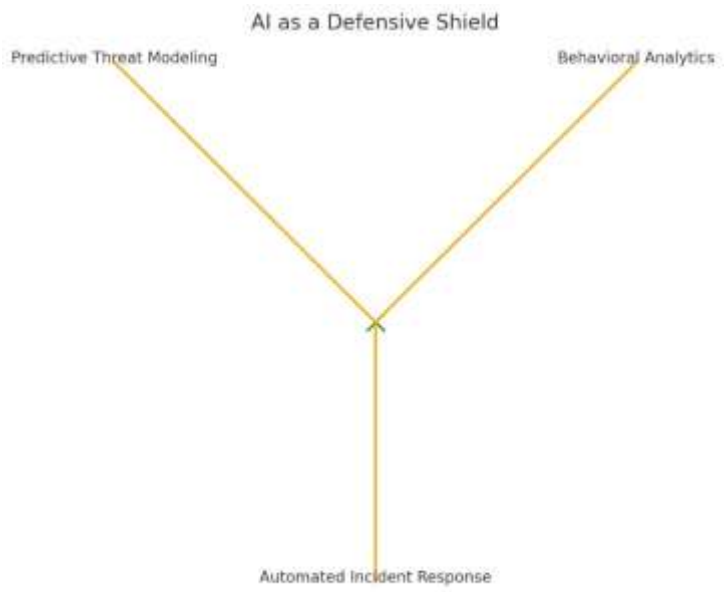

Figure 2: AI defence against cyber-attacks (Adopted from Kumar et al., 2023).

This article explore AI's dual role in cyber-security: how it has been used in recent breaches and how AI can be utilized in a responsible fashion. As AI powered threats are on the rise, understanding this is critical to building systems that are resilient to what comes next. The article further offers offer actionable insights by scrutinizing both risks and opportunities as organizations grapple with the ever changing and rapidly evolving scope of this landscape.

1.0 Recent Cyber-attacks and their Implications

The increasing reliance on digital systems and cloud infrastructures has escalated the frequency and severity of cyberattacks (Mohapatra and Reddy, 2024). For example, the recent Microsoft breach where attackers used credentials to access confidential data using cloud, these were simply cloud environment vulnerabilities that were exploited by the attackers (Kumar et al., 2021). The breach demonstrated the dire means by which cyber adversaries can cheaply weaponize advanced tool and tricks to attack critical systems. In fact, research attests that 98% of organizations have relationships with third parties that had suffered breach in last 2 years which prove that there are vulnerabilities of interconnected ecosystems in modern world (HIPAA, 2023). Moreover, a report shows that cyber-attacks with more than $1m losses has continued to increase across the years.

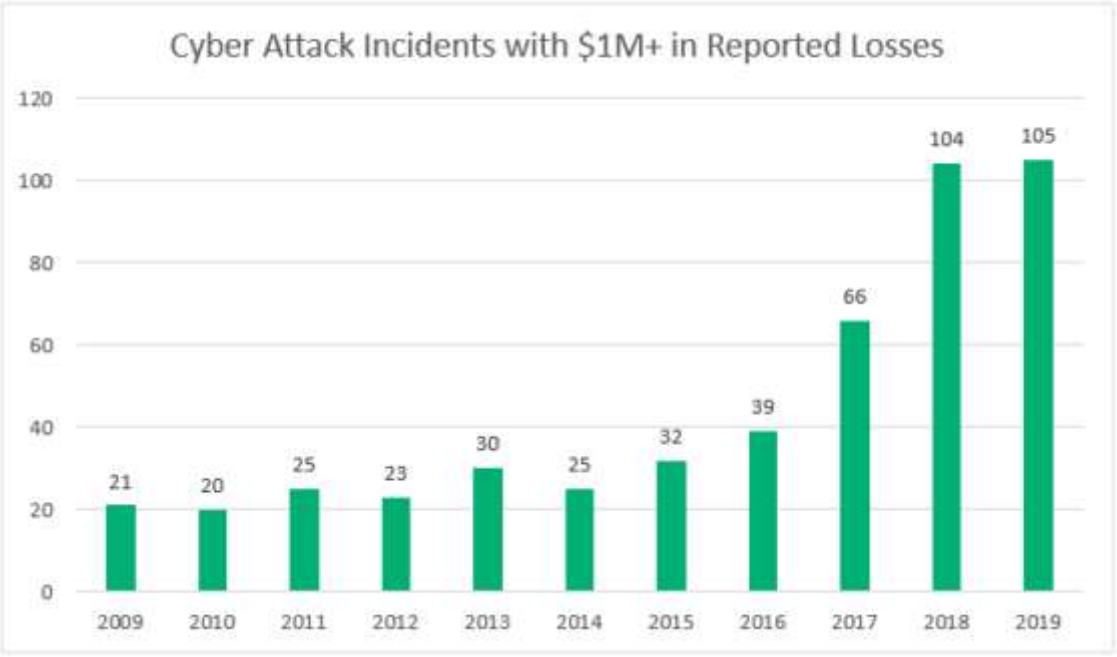

Figure 3: Rising losses on cyber-attacks over the years (Checkpoint, 2023).

Microsoft breach highlighted two primary implications: how cloud platforms are vulnerable and how automated tools can speed attack vectors (Jimmy, 2024). According to reports, attackers used very sophisticated tactics to exploit vulnerabilities in configurations that render even well secured environments vulnerable to targeted attacks (Aslan et al., 2023). This matches up with recent findings that security risks associated with cloud services have risen by 75% over the last year, posing significant challenges for businesses that rely on cloud services for scalability and flexibility (Security MEA, 2024).

Other high profile cyber incidents, including attacks such as targeting healthcare providers with ransomware, and Twitter breach help provide context to the systemic risk of cyber-attacks (Shafik, 2024). Social engineering tactics, powered by AI, can effectively circumvent technical safeguards by exploiting human vulnerabilities, the Twitter breach showed us (Fakhouri et al., 2024). Meanwhile, ransomware attacks demonstrate financial and operational impact of cyberattacks with the average ransom demand in 2023 exceeding $2 million, up from $400,000 in 2022 (Sophos, 2024).

These incidents reveal a troubling pattern: reconnaissance and exploitation attacks are increasingly automated, with attackers spending less and less time discovering weaknesses and executing attacks (Khan et al., 2024). With increased adoption of AI powered tools, it is easier for cybercriminals to launch personalized phishing campaigns, polymorphic malware, and real time

vulnerability scanning campaigns that put organisations of all sizes at risk. IBM's 2023 report also underscores the fact that downside detection tools that are too slow and hindered in advance cost organizations up to 32 percent more than those equipped with AI based threat detection tools (IBM, 2024a).

However, these trends have much broader implications beyond individual organizations out to the broader cybersecurity ecosystem. Small entities have a lack of cyber resilience, and the fact that attackers tend to use them as a point of entry to larger networks creates a cascading risk (Obi et al., 2024). With only 25% of small organizations carrying cyber insurance, compared to 75% among larger firms, the disparity in preparedness further exacerbates systemic vulnerabilities (World Economic Forum, 2024). To sum this up, latest cyber-attacks show not only the cloud vulnerability problem that needs to be addressed but also increasingly sophisticated AI-powered threats (Mallick and Nath, 2024). These incidents show how important it is for organisations to consider more complex defensive mechanisms like AI powered anomaly detection and automated incident response systems.

2.0 AI as a Tool for Cyberattacks

The execution of cyber-attacks has undergone a paradigm change with the arrival of artificial intelligence (AI) and increasingly sophisticated attacks have become more intentional, more scalable, and more evasive (Karthika et al., 2023). The implications are enormous, since AI contradicts traditional defensive strategies and articulates seemingly systemic deficiencies. Research by WEF (2024) shows that most leaders believe that cyber-attacks will increase particularly due to generative AI.

Industry	Percentage of leaders who think generative AI will most significantly affect cybersecurity in the next two years	Percentage of leaders who think their organizations are at least minimally cyber resilient
Cybersecurity	65%	94%
Agriculture, food and beverage	63%	38%
Banking and capital markets	56%	68%
Insurance and asset management	56%	89%
Professional services	53%	69%
Information technology and telecommunications	52%	81%
Health and healthcare and life sciences	46%	62%
Retail, consumer goods and lifestyle	44%	67%
Energy technology, energy utilities and oil and gas	41%	94%
Policy and administration	40%	60%
Education	33%	67%
Software and platforms	15%	77%

Figure 4: Sectors that leaders perceive will be affected by generative AI (WEF, 2023).

With the involvement of AI, these phishing campaigns had become more evolved and traditional, and yet, easily identifiable. Today, using AI models, attackers create as highly personalized phishing emails as possible, to boost luck (Baki et al., 2020). This precision comes from looking at huge datasets ranging from public information on social media to enabling attackers to trick people as if they are authentic contacts or institutions (Liu et al., 2021). An example of these is a Verizon (2024) report that shows that phishing (and AI driven campaigns) take place in several breaches. Such campaigns tip the scales for legitimate and malicious communication beyond the conventional tools which depend on static filters.

AI malware adapts its structure in real time to evade detection, an adaptation known as polymorphism (Manju and Rana, 2024). Unlike with traditional malware, that depends on static code signatures, AI driven malware changes its appearance and therefore signature-based detection is null and void. According to IBM's X-Force Threat Intelligence Index (IBM, 2024b), polymorphic malware has become a growing share of global attacks that use machine learning algorithms to bypass endpoint detection systems. This agility forces defenders to adopt behavior-based detection, which, while promising, remains resource-intensive and prone to false positives (Manju and Rana, 2024).

AI driven reconnaissance tools have cut down on the time to find vulnerabilities in systems (Guembe et al., 2022). These networks are scanned through tools which use machine learning to find misconfigurations, outdated software and exploitable pathways for attackers to isolate high value targets (Kaloudi and Li, 2020). This is an amplification of the efficiency for breaches we have seen in the Microsoft attack for example, where automated tools were heavily utilized to exploit cloud vulnerabilities. Such attacks are rapid, and defenders work at longer cycles, on the order of vulnerability assessment and patch deployment (Guembe et al., 2022). Evidence indicates that AI played a significant role in many high-profile breaches, including social engineering against Twitter (Siddiqi et al., 2022). Attacks succeeded at bypassing multi-factor authentication protocols with responses generated using natural language processing techniques that were indistinguishable from human operators (Beg et al., 2024). As with the Microsoft breach, we observe the lateral movement, but how AI can optimize an attacker's travel across compromised networks maximizing efficiency while unnoticed.

The weaponization of AI exposes a critical flaw in cybersecurity defences which is the technology gap between attacking and defending (Guembe et al., 2022). Both large organizations and smaller invest massively in AI driven defenses, but smaller entities lack the resources to counter such sophisticated threats, widening the preparedness divide (Liu et al., 2021). In addition, the ethical dilemmas concerning the dual use of AI should be elucidated since legitimate purposes designed tools which can further be co-opted for malicious use. These challenges need innovative technological solutions as well as regulatory frameworks to control how AI is used and to prevent it from being misused (Beg et al., 2024).

3.0 AI as a Defensive Shield

While AI has made cybercriminals much more sophisticated in their attack strategies, it has also changed the defensive game by giving organizations robust tools to fight those very threats (Kaloudi and Li, 2020). Its potential notwithstanding, integrating AI into cybersecurity is hindered by false positives, ethical dilemmas, cost barriers and hence strategic implementation is needed (Balantrapu, 2024).

Modern cybersecurity is built on AI powered behavioral analytics (Olabanji et al., 2024). AI analyzes user behavior and system activity, and looks for anomalies indicative of malicious activity (Olabanji et al., 2024). That means AI can be trained to respond to unexpected login times, unauthorized data transfer or deviations from usual workflows. The use of AI anomaly detection by organizations significantly reduces average breach detection time according to the Ponemon Institute (2024). However, a major difficulty is on balancing sensitivity against accuracy. If these systems are overly sensitive, they can generate false positives, or what we call "alert fatigue" among security teams. Predictive threat modeling is an opportunity for AI to use its ability to process vast datasets to identify potential vulnerabilities before they are exploited (Ajala et al., 2024). AI systems will be able to use historical attack patterns, emerging threat intelligence and organizational data to predict which attack vectors are likely and recommend corresponding preventative measures (Ajala et al., 2024). For example, a previous job required machine learning algorithms by companies like Palo Alto Networks detect risks from analysing billions of events daily to take action (Palo Alto, 2023). Yet, predictive models need constant fine tuning to remain viable, since cyber threats up their game quickly (Chowdhury et al., 2024).

The AI enabled automation of the traditionally time consuming process of incident response. Security Orchestration, Automation and Response or what is often abbreviated as SOAR tools enable organizations to spot and eradicate decreed threats as they happen (Kumari, 2024). For instance, an AI system to find a compromised endpoint in seconds instead of waiting for a compromised endpoint to move sideways across your entire network (Kumari, 2024).

Some companies have shown that AI can be utilized in cyber security (Chowdhury et al., 2024). One example would be that the financial sector heavily relies on AI to fight fraud – Mastercard's Interior Intelligence is a system that uses interfaces to track transaction patterns in order to foil any suspicious activity (Vieira, 2024). Like government agencies, AI is used by them to reinforce the security of critical infrastructure. But these successes are not common. However, small and medium enterprises (SMEs), which account for 43% or more of cyberattack victims, lack the resources necessary to deploy more advanced AI solutions and thereby widen the cybersecurity gap (Unger, 2021).

4.0 The Ethical Dilemma of AI in Cybersecurity

Artificial Intelligence's (AI) dual use nature is an ethical dilemma in cybersecurity. AI strengthens defenses, but so do evil actors – who repurpose and turn to their own good uses the systems by which we defend ourselves (Balantrapu, 2024). To address these issues, global collaboration and regulatory framework is required to make sure that we are using ethics and responsible AI. AI can analyze, predict, adapt, but this capability is being extended beyond any moral boundary by some people. The algorithms used to detect anomalies in networks are equally suitable to evade detection or exploit vulnerabilities (Camacho, 2024). An example is that AI driven tools for automating security penetration tests can be perverted by attackers to facilitate malicious reconnaissance (Perumal et al., 2024). According to research, most cybersecurity professionals believe that AI is making the race between attackers and defenders even more intense (Malatji and Tolah, 2024). The problem with unfortunate developers and the pitfalls of lax oversight being rooted in this dual use nature leave questions about responsibility (Perumal et al., 2024).

While democratizing AI tools increases innovation, sophisticated attackers are using this same democratization to launch advanced attacks, which puts power in the hands of less sophisticated actors (Kaloudi and Li, 2020). Open source AI models, designed to help push research forward, can be abused for the creation of very deep phishing campaigns, polymorphic malware and robotics for automated attacks (Balantrapu, 2024). These risks are the ethical dilemma that makes balancing the benefits of open access against the ethical risk of use. As an example, ChatGPT has been used to write believable phishing emails muddying the line between legitimate and malicious uses (CNET, 2023). WEF (2024) report in Figure 5 shows that most business leaders still believe

that AI will be more to the advantage of attackers than as a defence mechanism in the next two years. This strengthens the need for more regulation as to the usage.

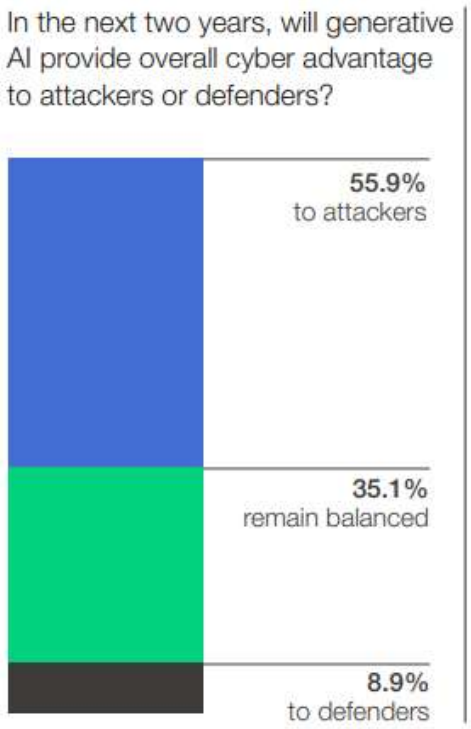

Figure 5: Responses on advantage of AI in 2 years (WEF, 2024).

AI systems anchor themselves into both attack and defense, accountability gets harder to define. Complicating things further is the opacity of much of which remains unknown to users of the system. However, transparency and explainability are under-developed in many of their applications, inhibiting accountability (Siddiqi et al., 2022).

Governments have to put in place more efforts to govern AI in cybersecurity. Frameworks such as the European Union's AI Act are designed to address high risk applications, but neglect the most pressing problems of AI in cybersecurity (Dhoni and Kumar, 2023). Creating enforceable standards requires international cooperation which is constrained by geopolitical tensions. Additionally, innovation must be balanced against security and ethical guidelines must strike a balance between the innovation and security and that defensive advances are not stifled without endangering AI from misuse (Feng et al., 2020).

A multi-faceted approach is needed to address these ethical dilemmas. Without these ethical aspects being embedded within an organization's systems, ethics must be the priority that's made. To do so, we need robust testing to keep users from using in unintended ways, secure development pipelines to minimize exploitation risks and cross-sector collaboration to share threat (Dhoni and Kumar, 2023). Additionally, governments, and other global bodies, must encourage international cooperation against global cyber threats, and agree to work towards meaningful regulatory frameworks which keep pace with ethical principles (Feng et al., 2020).

5.0 Call to Action: Building Resilient Systems

The escalating sophistication of AI-powered cyberattacks necessitates a proactive and collaborative approach to cybersecurity (Beg et al., 2024). Actionable recommendations for the integration of AI into cybersecurity frameworks, and possible challenges that could be posed by it are presented in this section.

Firstly, the, the zero trust model when combined with AI becomes more effective in that no entity is inherently trustworthy (Azad et al., 2024). The power of AI systems is in their ability to continuously analyze user behavior and access patterns, and then use dynamic access controls to enforce strict controls, and preempt potential breaches. Study show that reducing breach risks by 50% is possible through zero trust models with AI (Chaudhry and Hydros, 2023). But it comes with quite a bit of investment in AI capability, which smaller organizations may not have the means, however, public-private partnerships will be required to fill that gap (Chaudhry and Hydros, 2023). Moreover, cybersecurity infrastructure should include AI powered monitoring tools. These systems use machine learning to identify and cancel-out threats in real time: hours are replaced by seconds (Camacho, 2024). One example is that by integration of Security Orchestration, Automation, Response (SOAR) tools, Organizations can contain several of cyber threats without manual intervention (Dhoni and Kumar, 2023).

Finally, global action is also needed to combat cybersecurity, and it should be treated as a collective problem (Bechara and Schuch, 2021). To kick off international cooperation in establishing standards for the use of AI in cybersecurity, it is governments who should bring it on board (Trim and Lee, 2021). Organizations should be involved in threat intelligence sharing both to stay ahead of emerging risks and to invest in solutions that are actively minding your threat environment

(Bechara and Schuch, 2021). The World Economic Forum (2024), it's found that cybersecurity costs is significantly reduced due to collaborative initiatives.

Conclusion

AI plays both unprecedented challenges and opportunities in securing data in cybersecurity. It gives attackers the tools to conduct sophisticated breaches, and at the same time it provides defenders with the foundation of better detection, prevention, and response. The results presented prove that AI driven strategies, such as behavioral analytics, predictive modeling and real time incident response, can make a major difference to cyber resilience. But, these capabilities generate ethical dilemmas, gaps in accessibility and governance challenges that need immediate attention. To be able to build resilient systems, stakeholders must first give priority to innovation and collaboration. To keep pace with changing threats, it's important to integrate AI into zero trust architecture, encourage global cooperation, and deal with ethical considerations. Moreover, aligning defensive advances with ethical AI principles helps create responsible innovation. The onus to secure the digital landscape, with more and more developed by governments, organizations and technology developers, as we move from building AI-powered weapons to peaceful applications.

References

Ajala, O. A., Okoye, C. C., Ofodile, O. C., Arinze, C. A., & Daraojimba, O. D. (2024). Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time. *Magna Scientia Advanced Research and Reviews*, *10*(1), 312-320.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. https://www.mdpi.com/2079-9292/12/6/1333

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*, 101227. https://www.sciencedirect.com/science/article/pii/S2542660524001689

Baki, S., Verma, R. M., Mukherjee, A., & Gnawali, O. (2020). Less is more: Exploiting social trust to increase the effectiveness of a deception attack. *arXiv preprint arXiv:2006.13499*. https://arxiv.org/abs/2006.13499

Balantrapu, S. S. (2024). AI for Predictive Cyber Threat Intelligence. *International Journal of Management Education for Sustainable Development*, *7*(7), 1-28.

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359-374. https://www.emerald.com/insight/content/doi/10.1108/JFC-07-2020-0149/full/html

Beg, R., Bhardwaj, V., Kumar, M., Muzumdar, P., Rajput, A., & Borana, K. (2024). Unmasking Social Media Crimes: Types, Trends, and Impact. *Online Social Networks in Business Frameworks*, 1-26. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394231126.ch1

Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.

Chaudhry, U. B., & Hydros, A. K. (2023). Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. *IET blockchain*, *3*(2), 98-115. https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/blc2.12028

Checkpoint (2023). Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. Retrieved from: https://Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks - Check Point Blog

Chowdhury, R. H., Prince, N. U., Abdullah, S. M., & Mim, L. A. (2024). The role of predictive analytics in cybersecurity: Detecting and preventing threats. *World Journal of Advanced Research and Reviews*, *23*(2), 1615-1623.

CNET. (2023). *It's scary easy to use ChatGPT to write phishing emails.* Retrieved from https://www.cnet.com

Dhoni, P., & Kumar, R. (2023). Synergizing generative ai and cybersecurity: Roles of generative ai entities, companies, agencies, and government in enhancing cybersecurity. *Authorea Preprints*. https://www.techrxiv.org/doi/full/10.36227/techrxiv.23968809.v1

Fakhouri, H. N., Alhadidi, B., Omar, K., Makhadmeh, S. N., Hamad, F., & Halalsheh, N. Z. (2024, February). AI-Driven Solutions for Social Engineering Attacks: Detection, Prevention, and Response. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-8). IEEE. https://ieeexplore.ieee.org/abstract/document/10533010/

Feng, X., Feng, Y., & Dawam, E. S. (2020, August). Artificial intelligence cyber security strategy. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 328-333). IEEE.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial*

Intelligence, *36*(1), 2037254. https://www.tandfonline.com/doi/abs/10.1080/08839514.2022.2037254

HIPAA Journal. (2023). *98% of organizations use a vendor that had a data breach in the past 2 years.* Retrieved from https://www.hipaajournal.com/98-pc-organizations-vendor-data-breach/

IBM. (2024a). *Cost of a data breach report 2024.* Retrieved from https://www.ibm.com/reports/data-breach

IBM. (2024b). *X-Force Threat Intelligence Index 2024.* Retrieved from https://www.ibm.com/reports/threat-intelligence

Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 129-171. https://ojs.boulibrary.com/index.php/JAIGS/article/view/102

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1-34. https://dl.acm.org/doi/abs/10.1145/3372823

Karthika, C. V., Adhavan, N., & Pooja, S. J. (2023). Navigating the Perspective of Artificial Intelligence and Cybersecurity: Grabbing Opportunities amidst Ground Breaking Challenges. *Issue 4 Int'l JL Mgmt. & Human.*, *6*, 2702. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs24&section=237

Khan, O. U., Abdullah, S. M., Olajide, A. O., Sani, A. I., Faisal, S. M. W., Ogunola, A. A., & Lee, M. D. (2024). The Future of Cybersecurity: Leveraging Artificial Intelligence to Combat Evolving Threats and Enhance Digital Defense Strategies. *Journal of Computational Analysis and Applications*, *33*(8).

Kumar, M., Darshan, S. S., & Yarlagadda, V. (2023). Introduction to the cyber-security landscape. In *Malware Analysis and Intrusion Detection in Cyber-Physical Systems* (pp. 1-21). IGI Global. https://www.igi-global.com/chapter/introduction-to-the-cyber-security-landscape/331297

Kumar, S. U. B. O. D. H., Athavale, V. A., & Kartikey, D. I. V. Y. E. (2021). Security issues in cloud computing: A holistic view. *International Journal of Internet of Things and Web Services*, *6*, 18-29. https://www.iaras.org/iaras/filedownloads/ijitws/2021/022-0003(2021).pdf

Kumari, S. (2022). Cybersecurity in Digital Transformation: Using AI to Automate Threat Detection and Response in Multi-Cloud Infrastructures. *Journal of Computational Intelligence and Robotics*, *2*(2), 9-27.

Liu, M., Zhang, Y., Liu, B., Li, Z., Duan, H., & Sun, D. (2021). Detecting and characterizing SMS spearphishing attacks. In *Proceedings of the 37th Annual Computer Security Applications Conference* (pp. 930-943).

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*, 1-28.

Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1-69. https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf

Manju, & Rana, C. (2024). Application of Deep Reinforcement Learning in Adversarial Malware Detection. *Deep Reinforcement Learning and Its Industrial Use Cases: AI for Real-World Applications*, 91-113.

Mohapatra, A., & Reddy, G. (2024). The implications of Artificial Intelligence (AI) on cybersecurity: A detailed review for multidomain industry. *World Journal of Advanced Research and Reviews*, *23*(2). https://newsletter.radensa.ru/wp-content/uploads/2024/09/The_implications_of_Artificial_Intellige.pdf

Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: modern threats and advanced defense strategies. *Computer Science & IT Research Journal*, *5*(2), 293-310. https://fepbl.com/index.php/csitrj/article/view/758

Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science*, *17*(3), 57-74. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4709384

Palo Alto Networks. (2023). *From phishing to firewalls: Solving security with AI.* Retrieved from https://www.paloaltonetworks.com/blog/2023/06/solving-security-with-ai/

Ponemon Institute. (2024). *The 2024 study on the state of AI in cybersecurity.* Retrieved from https://ponemonsullivanreport.com/2024/04/the-2024-study-on-the-state-of-ai-in-cybersecurity/

Secureframe. (2024). *How will AI affect cybersecurity?* Retrieved from https://secureframe.com/blog/how-will-ai-affect-cybersecurity

Security MEA. (2024). *75% surge in cloud intrusions driven by identity-based attacks.* Retrieved from https://securitymea.com/2024/07/03/75-surge-in-cloud-intrusions-driven-by-identity-based-attacks/

Shafik, W. (2024). Cyber Attacker Profiling and Cyberbullying Overview. In *Cyber Space and Outer Space Security* (pp. 125-149). River Publishers. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003558118-5/cyber-attacker-profiling-cyberbullying-overview-wasswa-shafik .

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042. https://www.mdpi.com/2076-3417/12/12/6042

Sophos. (2024). *Ransomware payments increase 500% in the last year, finds Sophos state of ransomware report.* Retrieved from https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state

Trim, P. R., & Lee, Y. I. (2021). The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing*, *5*(3), 32. https://www.mdpi.com/2504-2289/5/3/32

Unger, A. (2021). *Susceptibility and Response of Small Business to Cyberattacks* (Master's thesis, Utica College).

Verizon. (2024). *2024 data breach investigations report.* Retrieved from https://www.verizon.com/business/resources/T22a/reports/2024-dbir-data-breach-investigations-report.pdf

Vieira, B. M. C. (2024). *Transforming finance: a VisionOS-Backed banking app with intelligent insights* (Doctoral dissertation).

World Economic Forum. (2024). *Widening disparities and growing threats cloud global cybersecurity outlook for 2024.* Retrieved from https://www.weforum.org/press/2024/01/wef24-global-cybersecurity-outlook-2024/