Issues in Information Systems
Volume 26, Issue 3, pp. 494-499, 2025

DOI: https://doi.org/10.48009/3_iis_2025_140

Revolutionary or evolutionary? An exploration of the role of AI in cybersecurity

Paul D. Nugent *Western Connecticut State University* nugentp@wcsu.edu

Abstract

This paper explores the uses of Artificial Intelligence (AI) in the subfields of cybersecurity. AI plays roles in threat detection and prevention, malware creation, security, and access control. The research question is whether these roles represent something revolutionary and unique, or whether they simply advance existing concepts and practices in an incremental fashion. The results of the analysis indicate that while AI is primarily making existing cybersecurity processes and practices more effective and efficient, it is doing so in a revolutionary manner.

Keywords: artificial intelligence, cybersecurity, access controls, risk management framework, malware creation

Introduction

This paper is an analysis of the various uses of Artificial Intelligence (AI) in the fields of cybersecurity. AI plays roles in threat detection and prevention, malware creation, security, and access control. The research question is whether these roles represent something revolutionary and unique, or whether they simply advance existing concepts and practices in an incremental fashion. Clearly, AI has succeeded in being a distinct new varietal of wine in many of the spheres discussed above. However, with the proliferation of AI into more specialized fields, such as cybersecurity, is it having the revolutionary impacts its proponents, and its popularity, seem to claim? This is an important question as the global price tag of AI-powered cybersecurity products exceeds $135 billion (Morgan, 2023). Given this flurry of excitement and investment, this paper explores to what extent it is truly introducing something novel, versus simply tweaking existing theory, technology, and practice.

Analysis

According to comprehensive reviews of the role of AI in cybersecurity, it is clear that AI primarily plays significant roles in four main areas: threat detection and prevention, malware creation, security, and access control (Francesco & Giacinto, 2023; Ansari et.al, 2022; Jada & Mayayise, 2024; Mendes & Rios, 2023; Naik et.al, 2022). The following sections explore each of these roles in more detail. Note, that this is largely a conceptual paper that explores the manner in which AI is altering the landscape of cybersecurity.

Threat Detection and Prevention

AI algorithms are used to detect threats to the confidentiality, integrity, and availability of information by analyzing threat-level data and comparing them against baseline levels or patterns (Cyber, 2024; Lundgren & Padyab, 2022; Francesco & Giacinto, 2023).

For example, in promoting their AI for threat detection and prevention, IBM focuses primarily on hybrid cloud environments and being more accurate in prioritizing threats (IBM, 2024). With respect to cloud protection, they state,

> AI tools can identify shadow data, monitor for abnormalities in data access and alert cybersecurity professionals about potential threats by malicious actors accessing the data or sensitive information—saving valuable time in detecting and remediating issues in real time. (IBM, 2024)

And for accuracy,

> AI-powered risk analysis can produce incident summaries for high-fidelity alerts and automate incident responses, accelerating alert investigations and triage by an average of 55%. The AI technology also helps identify vulnerabilities across threat landscapes and defend against cybercriminals and cyber crime. (IBM, 2024)

However, long before AI was a shiny new gem, Intrusion Detection Systems (IDPs) and Intrusion Detection and Prevention Systems (IDPSs) were widely used in organizations. These systems monitor volumes of files in storage as well as network traffic to look for suspicious patterns or levels of activity. Therefore, in this respect, the AI-aided detection systems mentioned above do nothing *functionally* new. Rather, AI makes these systems more efficient and effective through machine learning and predictive analysis to ascertain the likelihood of certain attacks, detect attacks, respond to attacks, and modify trigger levels (Shuba et. al., 2019; Siddiqi, 2020; Cyber, 2023; Frackiwicz, 2023; Jain et al., 2016; Koay, et. al., 2022).). Therefore, AI greatly automates and improves some of the processes that were previously performed by traditional IDPs, IDPSs, and human beings (Watkins, 2024; Shutenko, 2024).

Malware Creation

Malware represents malicious code such as viruses, worms, Trojan Horses, and logic bombs that can act like a legitimate user once they obtain access to the network system. Therefore, based upon the system privileges the malware is able to secure, it performs malicious actions such as deleting files, stealing files, manipulating files, and altering log files to hide or erase traces of its activity.

Over the years, this has created a cat-and-mouse game in which both the attacker and the hacker use similar tools and strategies to try to outsmart one another. Through white-hat hacking and penetration testing, organizations are able to discover vulnerabilities at the same time that black-hat hackers are feverishly trying to stay one step ahead. This dynamic continues with the introduction of AI. AI is able to generate computer code and is becoming a resource to produce increasingly sophisticated malware (Cyber, 2024; De Angelo, 2024).

As mentioned in the previous section, AI is very effective in characterizing threat actors and automating white-hat functions. This provides a basis from which AI can generate malware that equals or exceeds

existing threats. For example, a malware program called BlackMamba was created using AI and was able to get past strong detection systems such as Endpoint Detection and Response (EDR) in an experimental environment (Impact, 2023). According to this source, BlackMamba mutates every time it runs, making it more difficult for detection systems to recognize its pattern and,

> While the BlackMamba malware was only tested as a proof-of-concept and does not live in the wild, its existence does mean that the threat landscape for individuals and for organizations will be unequivocally changed by the use of AI. (Impact, 2023)

Another example involves shell malware (e.g., Bumble Bee Web Shell) which is a threat agent that AI was able to approximate with great accuracy (De Angelo, 2024; Falcone, 2021).

AI, then, takes the cat and mouse game to the next level, using machine learning, code generation, and mutation to potentially aid both the attackers and the defenders.

Security of AI systems

Cybersecurity Risk Management (RM) is a cost-benefit business approach to reducing cyber risk in organizations. Traditionally it attempts to use quantitative measures of asset value, probability of threats being successful, and effectiveness of controls to derive a quantitative level of risk that becomes the basis for deciding how to best invest in risk reduction. The goal of risk management is not to reduce risk to zero, which is virtually impossible as long as employees use the internet and email, but to reduce risk to an acceptable level in accordance with the organization's risk appetite.

The AI Risk Management Framework (NIST, 2024) playbook applies these RM activities to reduce risk associated with AI systems. This framework provides guidance on governance structures and policies, maps to better model AI systems, effective metrics and ongoing management processes (NIST, 2024). Therefore, in line with other types of technical systems, NIST and other policymakers have expanded their guidance to include AI systems (Comiter, 2019). Therefore, this does not address a direct role of AI in cybersecurity, but rather that the cybersecurity community deems AI to be a significant new form of technology requiring novel methodologies and risk management approaches.

Access control

Authentication and access control are fundamental facets of cybersecurity. They involve user identification, ensuring that the user is who they claim to be (authentication), and determining what the user will be able to do within the system (authorization). AI is now beginning play a role in enhancing these critical components. AI-based access controls transcend traditional username/password implementations. According to a recent source,

> AI is fundamentally changing access control by introducing automation, intelligence, and efficiency, making access control more accurate and real-time, while streamlining time-consuming tasks. AI can use internal and external data, raw historical data, and decision data to better understand patterns and context. (LenelS.2, 2024)

Some of the major elements in which AI is making contributions include data tracking and analytics, access accuracy, decision-making, visitor monitoring, task automation, system integration, and AI alarm systems (LenelS.2, 2024). For data analytics, AI can monitor access data to characterize user behavior,

> This can be combined with external data sources. This information can be used to identify potential threats and escalate them for investigation, for example, if an employee is accessing the building at unusual times or has been restricted due to changes in role or even external court orders or affiliations with competitors which can make that person a threat. Or it can also determine if that person's actions could result in a company, government or certification violation. For example, a person gaining access to handle a maintenance issue who does not have the proper prerequisite certifications and approvals could pose a personal threat to the individual and result in a violation or fine. (LenelS.2, 2024).

With respect to access accuracy, AI can enhance biometric authentication and,

> Combining biometrics with other forms of identity such as card or mobile credentials can provide higher accuracy and determine that the person gaining access is not using someone else's credentials. This is because AI and Deep Learning techniques can recognize patterns and identify individuals more reliably than other non-biometric-based credentials. (LenelS.2, 2024).

Many of these key themes are also addressed in the collection of essays in *AI for Cybersecurity: Robust models for Authentication, Threat and Anomaly Detection* (Francesco & Giacinto, 2023) but do not introduce strong arguments that AI is doing anything functionally new. AI simply performs these functions more efficiently and effectively than traditional approaches.

Conclusions

While the analysis is not an exhaustive treatment of all instances of AI's role in cybersecurity, it nonetheless reflects the most important areas. In answering the research question, the analysis is somewhat divided. On the one hand, AI has not changed the basic tenets of cybersecurity. Threats to the confidentiality, integrity, and availability of information continue to be the main focus and risk management techniques continue to monopolize a business-centered approach to reducing risk. Therefore the "old bottles" haven't changed in theory – AI introduces few new features with the possible exception of machine learning. On the other hand, AI is such a powerful analytic tool that it acts like a steroid for existing functional cybersecurity techniques and practices. In this respect, the "new wine" is potent enough to warrant the claim that AI represents a revolutionary turning point in cybersecurity. Future research on this theme should include empirical evidence regarding the degree to which cybersecurity processes are improved based on the application of AI services.

References

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of Advanced Research in Computer and Communication Engineering.*

Comiter, M. (2019). Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. *Belfer Center for Science and International Affairs. Belfer Center for Science and International Affairs*. Retrieved 12/20/2024 from https://www.belfercenter.org/publication/AttackingA

Cyber (2024). *Risks of AI & Cybersecurity: Risks of artificial intelligence*. Malwarebytes. https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security.

De Angelo, D. (2024). The Dark Side of AI in Cybersecurity — AI-Generated Malware. Retrieved 12/19/2024 from https://www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/#:~:text=The%20Shifting%20Landscape%20of%20Cybersecurity&text=He%20further%20predicts%2C%20%22AI%20will,and%20be%20much%20more%20effective.%22

Falcone, R. (2021). xHunt Campaign: New BumbleBee Webshell and SSH Tunnels Used for Lateral Movement. Retrieved 12/20/2024 from https://unit42.paloaltonetworks.com/bumblebee-webshell-xhunt-campaign/

Frąckiewicz, M. (2023, June 6). The ethics of OpenAI's AI integration in the workplace: Addressing human labor rights and dignity. *TS2 SPAC*E. Retrieved 12/19/2024 from https://ts2.space/en/the-ethics-of-openais-ai-integration-in-the-workplace-addressing-human-labor-rights-and-dignity/

Francesco, B., & Giacinto, G. (Eds.) (2023). AI for Cybersecurity: Robust models for Authentication, Threat and Anomaly Detection. *Basel: MDPI - Multidisciplinary Digital Publishing Institute.*

IBM (2024). Artificial intelligence (AI) cybersecurity. Retrieved 12/24/2024 from https://www.ibm.com/ai-cybersecurity?utm_content=SRCWW&p1=Search&p4=43700074604519875&p5=p&p9=58700008209812892&gclid=EAIaIQobChMIjJ3L5pLSiQMVJWBHAR0o3RmxEAAYASAAEgIKqvD_BwE&gclsrc=aw.ds

Impact (2023). AI-Generated Malware and How It's Changing Cybersecurity. Retrieved 12/18/2024 from https://www.impactmybiz.com/blog/how-ai-generated-malware-is-changing-cybersecurity/

Jada,I., & Mayayise, T. O. (2024). "The Impact of Artificial Intelligence on Organisational Cyber Security: An outcome of a systematic literature review," *Data and Information Management* 8.

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big Data Privacy: A Technological Perspective and Review. *Journal of Big Data, 3*(1). Retrieved 12/20/2024 from https://doi.org/10.1186/s40537-016-0059-y.

Koay, A. M. Y., Ryan, K. L., Ko, H. H., & Radke, K. (2022). Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*. Retrieved 12/20/2024 from https://doi.org/10.1007/s10844-022-00753-1.

LenelS.2. (2024). 7 Ways AI is Changing Access Control & Security. Retrieved 12/15/2024 from https://www.lenels2.com/en/news/insights/7_ways_ai_is_changing_access_control.html

Lundgren, M., & Padyab, A. (2022). A review of Cyber Threat (Artificial) Intelligence in Security Management. *Artificial Intelligence and Cybersecurity*, 29–45. Retrieved 12/20/2024 from https://doi.org/10.1007/978-3-031-15030-2_2

Mendes, C. & Rios, T. N. (2023). "Explainable Artificial Intelligence and Cybersecurity: A Systemic Literature Review." *Cornell University: Computer Science>Cryptography and Security.* https://arxiv.org/abs/2303.01259

Morgan, S. (2023, September). *AI and Cybersecurity: A New Era*. Morgan Stanley. Retrieved 12/20/2024 from https://www.morganstanley.com/articles/ai-cybersecurity-new-era

Naik, B., M, A., Yagnik, H., & Shah, M. (2022). The Impacts of Artificial Intelligence Techniques in Augmentation of Cybersecurity: A Comprehensive Review. *Complex & Intelligent Systems.* 2022-04, Vol. 8 (2).

NIST. (2024). NIST AI RMF Playbook. Retrieved 12/20/2024 from https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook#:~:text=NIST%20AI%20RMF%20Playbook&text=Suggestions%20are%20aligned%20to%20each,Map%2C%20Measure%2C%20Manage)

Siddiqi, S. (2020). Leveraging Artificial Intelligence for Cybersecurity: Trends, Opportunities, and Challenges. *International Journal of Network Security & Its Applications (IJNSA). 12*(5). https://doi.org/10.5121/ijnsa.2020.12503

Shuba, C. A., et al. (2019). Application of Artificial Intelligence for Cyber Security: A Comprehensive Review. *IEEE Access, 7, 10151-10176*. Retrieved 12/20/2024 from https://doi.org/10.1109/ACCESS.2018.2886377

Shutenko, V. (2024, March 15). AI in cyber security: Top 6 use cases. *TechMagic*. Retrieved 12/20/2024 from https://www.techmagic.co/blog/ai-in-cybersecurity/

Stanham, L. (2023, November 3). Machine Learning in Cybersecurity: Benefits and Use Cases | CrowdStrike. *Crowdstrike.com*. Retrieved 12/17/2024 from https://www.crowdstrike.com/cybersecurity-101/machine-learning-cybersecurity

Watkins, O. (2024, April 19). 4 Use Cases for AI in Cyber Security. Retrieved 12/20/2024 from https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security