KAUTILYA
SCHOOL OF
PUBLIC POLICY

Issue Brief Series

AI and its Impact on Cybersecurity

Issue Brief Number: IB-2025-15

Submitted by: Mr. Vivek Kalhan Reshi Raina (MPP Cohort 2023-25)

Under the Guidance of: Dr. Vishnu S. Pillai, Assistant Professor at Kautilya School of Public Policy

Cite this Article as *Raina, V. K. R. (2025). AI and its Impact on Cybersecurity. Kautilya School of Public Policy [online]. Available at: https://kspp.edu.in//issue-brief/ai-and-its-impact-on-cybersecurity*

AI and its Impact on Cybersecurity

Executive Summary

The integration of Artificial Intelligence (AI) in the arena of cybersecurity denotes a transformative shift in how organizations have started to protect their digital assets. As cyber threats evolve and become sophisticated in nature, traditional cybersecurity measures are proving to be inadequate. AI on its part, enhances threat detection, response, and overall defense mechanisms by analyzing vast datasets to identify patterns suggestive of potential breaches. The market share of AI in cybersecurity has been projected to grow significantly, with a compound annual growth rate of 21.9% from 2023 to 2028, thereby throwing light on its growing role as a modern security strategy. As with any other technology though, the dual nature of AI as both a defensive and offensive tool introduces complex risks, including the potential for AI-driven cyberattacks. This paper explores the applications of AI in cybersecurity, examines the implications for various stakeholders, and discusses the associated risks and challenges.

Sector and Sectoral Applications

Explanation of the Sector of Interest

Cybersecurity as per Cisco, is the "practice of protecting systems, networks, and programs from digital attacks." These attacks are intended to access, change or destroy sensitive information, extort money from users or interrupt routine business processes (*Cisco Security: A Better Way of Doing Security.*, 2024). The increasing dependence on digital infrastructure across the spectrum of the industries has made robust cybersecurity measures important. According to Craigen et al. (2014), cybersecurity protects private information and ensures service availability in an era where cyber threats are inescapable. The sector encompasses various domains including

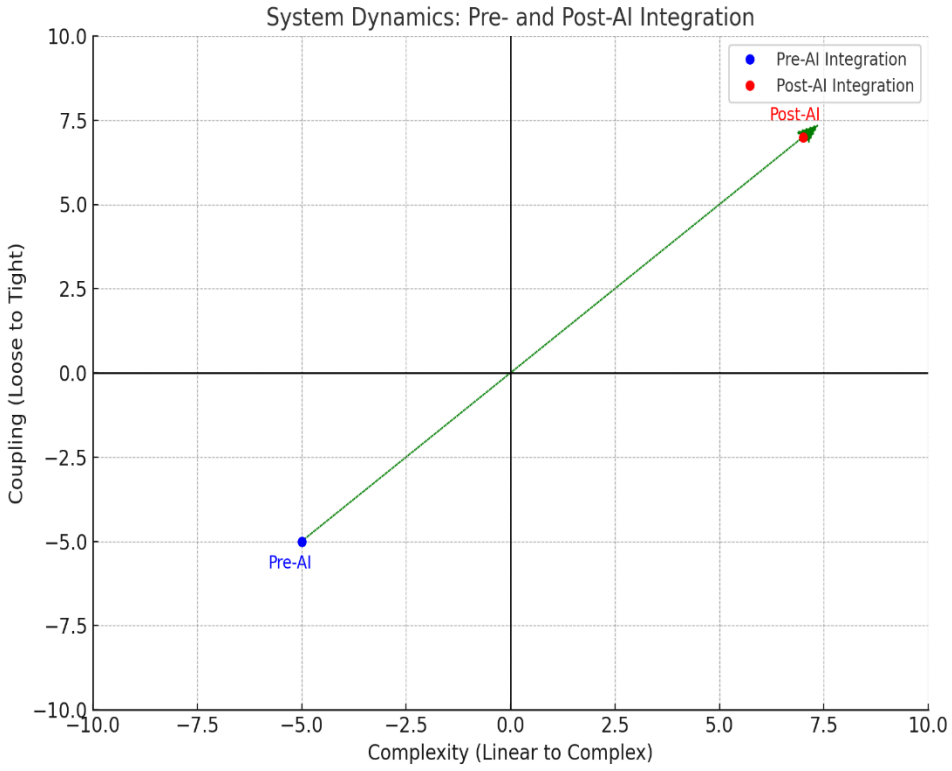
network security, application security, information security, and operational security (Kaspersky, no date).

Potential for AI Application in the Sector of Interest

AI's potential in cybersecurity is substantial due to its ability to process large volumes of data rapidly and identify patterns that humans might find difficult to handle at once. AI technologies such as machine learning (ML) and deep learning have the capability to detect threat by analyzing user behavior and network traffic in real-time (Bhatele et al., 2019). For example, AI can automate the identification of anomalies symptomatic of cyber threats, thereby improving response times and reducing the burden on human-centered cybersecurity teams (IBM, 2023). The projected growth of the AI market in cybersecurity underscores its potential: it is expected to reach $60.6 billion by 2028 (Polito & Pupillo, 2024).

Systems Perspective: Change in Complexity and Coupling

As per Perrow (2011), complexity means unanticipated interactions, unintended interactions or intended but unfamiliar (infrequently used systems) ones. Artificial Intelligence integrated with cybersecurity will introduce new complexities and coupling dynamics within systems. Traditional cybersecurity frameworks often operate on predefined rules and require active human involvement at every stage; however, AI-enabled systems adaptively learn from ongoing data interactions (Kaur et al., 2023). This feature of adaptability increases system complexity as AI models require continuous updates and training to remain effective against evolving threats (Kaur et al., 2023). The following diagram explains the change in coupling and complexity.



In addition to the complexity, the coupling between AI systems and existing cybersecurity protocols requires careful re-design to avoid vulnerabilities that could be exploited by adversarial actors. As such, organizations must navigate this intricate landscape while ensuring that their defenses are robust against both conventional and AI-enhanced attacks.

Discussion on the Potential Risks and Impact Groups

Impact Groups of Diverse AI Applications

The different applications of AI in cybersecurity can impact various stakeholders differently in their field (Kumar & Niharika, 2024). They can be grouped as such:

Organizations (Impact Group 1) – Businesses will look to leverage AI in order to enhance cybersecurity breach and threat detection as well as response capabilities (Saied et al., 2023). As such, AI in cybersecurity impacts them directly.

Cybercriminals (Impact Group 1) – Adversarial actors in the network will also look to exploit AI technologies to aim their cyber-attacks in a better manner (Sultan & Sultan, 2024). But they too will have to face improved cybersecurity checks to execute their attacks (Sultan & Sultan, 2024).

Cybersecurity professionals (Impact Group 2)- Cybersecurity teams and professionals will also benefit from AI-driven automation of vulnerability and risk management aspects of cybersecurity measures (Morovat & Panda, 2020).

End users/ Individual users (Impact Group 3) - Consumers will be affected on both ends, being helped by improved cybersecurity measures but will also be exposed to potential AI-driven cyber-attacks as well risks of potential privacy breaches due to constant monitoring by AI systems.

Defense Industrial Complex (Impact Group 4) – Going into the future, scaled AI implementation in cybersecurity has the potential to impact how a country's defense organization adapts to cyber-attacks that are commonplace right now, but are sure to increase in intensity and volume with the integration of AI (Cohen, 2023).

Impacts of Technology Interventions on Impact Groups

The stakeholder groups mentioned in the previous section will face multi-faceted effects with the intervention of AI technologies:

Organizations – Improved threat detection capabilities will lead to reduction in incident response time. However, the dependency created on AI-driven automated systems is bound to create complacency among cybersecurity teams (Saied et al., 2023).

Cybercriminals – AI-powered tools in the hands of cybercriminals can lead to more targeted and damaging attacks from their end (Sultan & Sultan, 2024). On the other end of the spectrum though, they will have to beat the AI defense systems in order to break into a secure digital environment (Sultan & Sultan, 2024).

Cybersecurity Professionals – With AI-driven automation, efficiency of cybersecurity professionals is bound to go up. But it will raise questions about job displacements and the need to upskill continuously in order to manage cybersecurity incidents in an effective manner (Morovat & Panda, 2020).

End users/ Individual users – Improved security measures can lead to increased trust in digital services; however, privacy concerns may arise from extensive data collection practices inherent in many AI systems (Bhatele et al., 2019)

Defense Industrial Complex – AI's potential is humongous in defense industry's cyberspace. It can help in the fight against cyber threats faster than traditional methods, helping to uncover signs of cyber-espionage and sometimes even preempting cyber-attacks (Cohen, 2023).

.

References

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In *Advances in digital crime, forensics, and cyber terrorism book series* (pp. 170–192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

Cisco Security: A better way of doing security. (2024, November 1). [Video]. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html#:~:text=Cybersecurity%20is%20the%20practice%20of,or%20interrupting%20normal%20business%20processes.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, *4*(10), 13.

IBM. (2023). The future of cybersecurity: How AI is transforming security operations. Retrieved from https://www.ibm.com/security/artificial-intelligence

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kumar, N. A., & Niharika, K. (2024). Stakeholder Perspectives On The Influence Of Artificial Intelligence In E-Governance And Cybersecurity For Smart Cities. *International Journal of Engineering Science and Advanced Technology.*, *24*(10), 379–387. https://doi.org/10.36893/ijesat.2024.v24i10.048

Morovat, K., & Panda, B. (2020). A survey of Artificial Intelligence in Cybersecurity. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 109–115. https://doi.org/10.1109/csci51800.2020.00026

Polito, C., & Pupillo, L. (2024). Artificial intelligence and cybersecurity. *Intereconomics*. https://www.intereconomics.eu/contents/year/2024/number/1/article/artificial-intelligence-and-cybersecurity.html

Perrow, C. (2011). *Normal Accidents: Living with High Risk Technologies-Updated Edition*. Princeton university press.

Saied, M., Guirguis, S., & Madbouly, M. (2023). Review of artificial intelligence for enhancing intrusion detection in the internet of things. *Engineering Applications of Artificial Intelligence*, *127*, 107231. https://doi.org/10.1016/j.engappai.2023.107231

Sultan, M. S., & Sultan, M. S. (2024). Leveraging Artificial intelligence for Enhanced Cybersecurity: A Systematic approach. *International Journal of Science and Research (IJSR)*, *13*(8), 832–839. https://doi.org/10.21275/sr24812100704

Kaspersky (no date). What is Cybersecurity? Types, Threats and Cyber Safety Tips. *Kaspersky.* https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security