Chapter 11
AI-Driven Cyber Threats: Behavioral Analysis and Strategic Defenses

Turki Fahed Al Masaeid
http://orcid.org/0000-0002-7901-5656
Abu Dhabi School of Management, UAE

ABSTRACT

The behavioural analysis of AI attacks is of extreme significance in contemporary-day cybersecurity as it pertains to how AI has the potential to enhance or disrupt security measures. AI attacks use leading-edge machine learning, deep learning, and natural language processes to carry out sophisticated attacks. AI defences, on their part, use predictability analysis and anomaly detection to counter attacks. In this chapter, AI in cybersecurity has dual responsibilities in threat reaction, reaction, and adaptation mechanisms. AI-based adversarial AI attacks, AI-based social engineering attacks, and AI-based automated exploitation attacks have been elucidated together with AI-based defences such as behavioural profiling and self-healing mechanisms. Real-life scenarios have been presented in the chapter to elucidate how AI has contributed to or has been employed in cyber wars.

INTRODUCTION

Background and Context

The emergence of artificial intelligence (AI) has significantly changed the models of digital security, both by creating previously unachieved defensive capabilities as well as creating new vulnerabilities. AI-enabled technological innovations, including machine learning (ML), deep learning (DL), and natural language processing

DOI: 10.4018/979-8-3373-6801-6.ch011

(NLP), have significantly expanded threat identification and management, says Ali et al. (2025). However, the two-fold utilization of AI has also witnessed AI-enabled attacks, wherein attackers use AI capabilities to outwit traditional security. Also, AI's capacity to perform very evasive and adaptive cyberattacks further enhances the threat environment. AI threats, as indicated by Alanezi and Al-Azzawi (2024), employ sophisticated strategies such as phishing, adversarial attacks, and social engineering through deepfakes, rendering it more challenging for traditional security protocols. AI-generated phishing emails, for instance, are able to bypass email filters by simulating human language patterns, targeting users' psychology.

From an organizational behavior perspective, AI-powered threats involve complex issues regarding human decision-making processes, as well as conformity in terms of security. According to Yzzogh et al. (2024), the success of cybersecurity does not only depend on technological means, but also organizational adaptability, employee behavior, and security culture. The increased emphasis by security on AI necessitates an approach that involves human-AI interfaces so that secure, adaptive models of cybersecurity are developed (Guembe et al., 2022). In general, AI-enabled threat advancement highlights the importance of an interdisciplinary approach, marrying AI-enabled defence strategies with an extensive examination of human behavioural patterns in cybersecurity.

Defining Behavioural Analysis in Cybersecurity

Behavioural analysis in computer security involves analyzing systematically users' behavior, anomalies, and threat actors' behavioural patterns so as to uncover and contain threats. Olabanji et al. (2024) explain AI-driven behavioural analysis employs ML models to monitor deviation from normal users' behavioural patterns, identifying potential threats through the use of anomaly models. Existing strategies toward computer security rely on rule-based models, which are static when it comes to adjusting to dynamically evolving threats. AI-driven strategies, by way of contrast, employ behavioural data in real time so as to enhance predictive capacity.

Behavioural analysis comes very handy while battling AI threats, which constantly change form so as not to get detected. AI behavioural analysis, says Shankari and Rethinavalli (2024), surpasses other other traditional methods when it comes to predictive analysis, enabling organisations to anticipate threats even before occurrence. AI-powered systems, for instance, are able to monitor login patterns, keystrokes, and device usage patterns so as to flag account takeovers, insider threats, or other suspicious work environment incidents.

However, traditional strategies have an important role to play in gaining cybersecurity resilience. Singh et al. (2024) clarify that traditional defence strategies, such as firewalls, intrusion detection system (IDS), provide fundamental defence layers.

An Improved Disc Segmentation Based on U-Net Architecture for Glaucoma Diagnosis

Radia Touahri, Nabiha Azizi, Nacer Eddine Hammami, Farid Benaida, Nawel Zemmaland Ibtissem Gasmi (2022). *International Journal of Ambient Computing and Intelligence (pp. 1-18).*

www.irma-international.org/article/an-improved-disc-segmentation-based-on-u-net-architecture-for-glaucoma-diagnosis/313965