AI: Double-Edged Sword of Cybersecurity

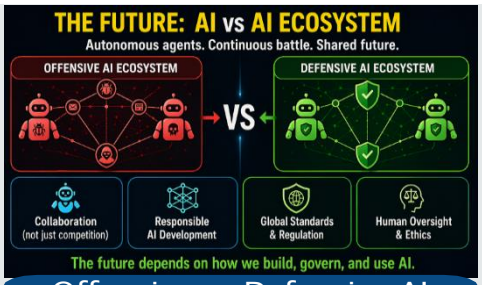
Dr. Shapla Khanam, Department of AI, FSCIT

Artificial Intelligence (AI), from an initial tool for Data Analytics, is evolving into an autonomous tool that supports sophisticated cyber-attack and defence. This raises ethical concern which using AI for Strong Shield as a defence and attacking tool.

Nowadays, the cybercriminals were no longer limited to manual attack or static malware. With the implementation of AI in the Cybercriminal Industry, it enables system to perform automated reconnaissance, exploit and identify system vulnerabilities at a massive scale. While the Generative AI model can generate highly realistic phishing email to tailored to a targeted individual or Organization.

On the other side of the battlefield, defenders are leveraging AI to encounter the growing threat by implementing Autonomous Defence. Those Autonomous Defence Systems can provide monitor massive volumes of network traffic, detect anomalies, and respond to incidents within milliseconds ways much faster than any human manual detection. This shift from reactive to predictive security represents one of the most significant advantages AI brings to the cybersecurity industry.

The rise of the implementation of Autonomous AI in the cybersecurity sector also raises serious ethical concerns. Where the systems that operate independently can make major mistakes, which potentially disrupt legitimate organization operations and escalate conflicts unintentionally due to the decision of AI. While there is also the risk of adversarial AI Systems that are designed specifically to deceive or manipulate defensive algorithms.



Offensive vs Defensive AI

To navigate into a new reality, private organizations and government must invest and putting effort in AI literacy alongside with fast growing Cybersecurity technology. By deep diving into how Autonomous AI systems work on Cyber Défense and their trade-off. The collaboration between varies bodies in industry, governments, and academia will be key to establishing standards, sharing threat intelligence and developing ethical framework for using AI in the neutral, offensive and defensive Cyberoperation System.

AI As Both Weapon & Defense: The Rise of Autonomous AI in Cybersecurity

Contact at: shapla.k@um.edu.my