CENTRE FOR JOINT WARFARE STUDIES

GL/9/25

USE OF AI IN CYBERCRIME AND CYBER SECURITY

BY

BRIG SAURABH TEWARI (RETD)

ORGANISED BY CENJOWS
20TH FEB 2025

USE OF AI IN CYBER CRIME AND CYBER SECURITY
BY BRIG SAURABH TEWARI (RETD)
ORGANISED BY CENJOWS ON 20 FEBRUARY 2025

Artificial Intelligence (AI) is revolutionising human activities as well as, shaping business, security, and everyday life. With advancements in Machine Learning (ML), Deep Learning, Large Language Models (LLMs), Natural Language Processing (NLP), and Generative AI (Gen-AI), AI is surpassing human capabilities. However, its misuse is rising, with cybercriminals exploiting AI for deepfake creation, voice cloning, phishing, and malware development. At the same time, AI strengthens cybersecurity by enabling predictive threat detection, automated incident response, and forensic investigations. The growing influence of AI presents both opportunities and challenges, making it necessary to understand its implications on cybercrime and cybersecurity.

Use of AI in Cybercrime

AI has significantly altered the cybercrime landscape, allowing even non-technical individuals to execute large-scale frauds. Cybercriminals exploit AI-driven tools, such as ChatGPT, to conduct scams remotely. Key AI applications in cybercrime include:

- **Deepfake Videos & Voice Cloning.** AI generates fake videos and audio, enabling fraud and misinformation.
- **Social Engineering Attacks.** AI-driven phishing emails deceive individuals and organisations.
- **Password Cracking.** AI algorithms crack passwords faster than conventional techniques.
- **Automated Malware Creation.** AI helps criminals generate complex malware without coding knowledge.
- **Adversarial Attacks.** Attackers manipulate AI models via data poisoning.
- **Polymorphic Malware.** AI generates self-modifying malware that evades detection.

- **Ransomware Attacks.** AI automates ransomware execution, making attacks more effective.

As AI evolves, cybercriminals will develop increasingly more sophisticated threats and thereby making mitigation more challenging.

Use of AI in Cybersecurity

Despite its risks, AI is a critical tool for cybersecurity, helping organisations proactively detect and counter cyber threats. AI applications in cybersecurity include:

- **Threat Intelligence & Predictive Mitigation.** AI predicts cyber threats and strengthens defences.
- **Offensive Security Testing.** AI identifies vulnerabilities before attackers can exploit them.
- **Automated Incident Response.** AI isolates compromised systems and triggers alerts.
- **DDoS Attack Detection.** AI analyses network activity to detect and mitigate attacks.
- **Bot Identification.** AI distinguishes between good and malicious bots.
- **Advanced Malware Detection.** AI enhances the identification of evolving malware threats.
- **Forensic Investigations.** AI aids in tracking and analysing cybercrimes.
- **Facial Recognition for Law Enforcement.** AI-powered tools assist in criminal identification.
- **Deepfake & Voice Cloning Detection.** AI helps detect fake media content.
- **Social Engineering & Spam Detection.** AI mitigates phishing and fraudulent schemes.

By integrating AI, cybersecurity professionals can proactively combat cyber threats and prevent potential breaches before they cause widespread damage.

Challenges in AI Adoption

AI adoption presents technological, ethical, social, and legal challenges. AI relies on vast data sets, raising concerns about data privacy, security, and biases. High computational power and validation mechanisms are required for accuracy. Additionally, the legal framework is inadequate to address AI-driven security risks, necessitating new laws to regulate AI ethics and prevent misuse. The lack of global standardisation makes AI regulation even more complex.

Conclusion

AI is a double-edged sword, fuelling both cybercrime and cybersecurity. As AI advances, cybercriminals will develop more sophisticated attacks, posing greater challenges for cybersecurity professionals. To ensure AI serves humanity positively, a robust regulatory framework and ethical AI governance are essential. Without stringent regulations, AI-driven cyber threats will escalate, making global cooperation critical in securing the digital landscape and ensuring AI is used for ethical and constructive purposes.