

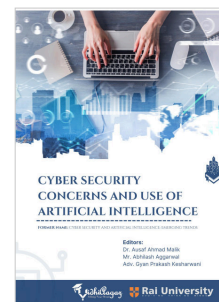
CHAPTER 39

The Role of Artificial Intelligence in Cyber Crime

Mandeep Sharma and Nitu

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 335–338

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Mandeep Sharma & Nitu, *The Role of Artificial Intelligence in Cyber Crime*, in CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE 335 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Mandeep Sharma and Nitu, ‘The Role of Artificial Intelligence in Cyber Crime’ in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 335.

CHICAGO (17TH ED.)

Sharma, Mandeep, and Nitu. “The Role of Artificial Intelligence in Cyber Crime.” In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 335–338. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-39/>.

APA (7TH ED.)

Sharma, M., & Nitu. (2024). The role of artificial intelligence in cyber crime. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 335–338). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-39/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-39/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER CRIME

Mandeep Sharma⁷³ and Nitu⁷⁴

ABSTRACT

Artificial Intelligence (AI) is a popular term in the cyber world. It is still an emerging science in many areas in response to the problems of the twenty-first century. Artificial intelligence is now inextricably linked to human existence. Today, it is impossible to envision a future without AI since technology has such a profound influence on human existence. The primary goal of AI is to construct technology-based activities that represent human knowledge in order to solve issues. Simply put, AI is the study of how people think, work, learn, and make decisions in all aspects of life, whether it's problem solving, learning new things, thinking rationally, arriving at a solution, and so on. AI is in every area of human life, naming a few it is into gaming, language processing, speech recognition, expert system, vision system, hand writing recognition, intelligence robots, financial transactions and what not, every activity of human life has become a subset of AI. In spite of numerous uses, AI can also be used for destroying the human life, that is the reason human inference is required to monitor the AI activities. Cybercrime has become commonplace, with regular news coverage. It is a problem that affects the whole world, not just one country. Without solid security measures, AI is pointless since it is easily accessible to others. Hacker-led cyber attacks have posed a significant danger to governments, banks, and global corporations. Hackers exploit a large volume of individual and organisational data, posing a significant danger to the cyber world. In this regard, research in the fields of AI and cyber security has grown in importance in recent years, and it will continue to do so indefinitely since it is a dynamic and sensitive topic related to human existence.

Keyword: artificial intelligence , cyber crime, cyber security,

INTRODUCTION

Artificial Intelligence (AI) refers to the development of computer systems capable of performing tasks that typically require human intelligence. These tasks include learning from experience, reasoning, problem-solving, language understanding, perception, and even creativity. AI aims to create machines that can mimic or exceed human cognitive abilities, offering vast potential in various fields such as healthcare, finance, robotics, transportation, and beyond.

AI technologies are driven by algorithms, machine learning (ML), and data processing. Machine learning, a subset of AI, enables systems to improve and adapt autonomously by analyzing large datasets and recognizing patterns. Over the years, AI has rapidly evolved, moving from theoretical research to real-world applications that shape industries and everyday life.

Artificial intelligence (AI) plays a significant role in both enhancing cybersecurity and contributing to cybercrime. While AI offers powerful tools for defending against cyber threats, it is also being used by cybercriminals to carry out more sophisticated attacks. Here's a breakdown of AI's dual role in this context:

AI's Role in Cybercrime (Offensive Use by Cybercriminals):

1. **Automated and Scalable Attacks:** AI enables cybercriminals to automate large-scale attacks,

⁷³ Research Scholar at Chaudhary Devi Lal University, Sirsa, India.

⁷⁴ LLM Scholar from Chhaju Ram Law College, Hisar, India.

allowing them to target many victims simultaneously with minimal human intervention. Techniques like AI-powered bots can scan networks for vulnerabilities, execute phishing campaigns, or launch Distributed Denial of Service (DDoS) attacks more efficiently than manual efforts.

2. **Advanced Phishing and Social Engineering:** AI enhances phishing attacks by analyzing vast amounts of personal data to craft more personalized, convincing messages. AI systems can mimic human communication patterns, making phishing emails or social engineering attempts much harder to detect. This leads to a higher success rate for attacks that aim to steal sensitive information or login credentials.

3. **Sophisticated Malware Creation:** AI can assist in the development of malware that adapts and evolves based on the target environment. AI-enhanced malware can evade traditional security measures by learning from its surroundings and adjusting its behavior to avoid detection. Examples include polymorphic malware, which changes its code to elude antivirus systems, and ransomware that selectively targets high-value files for encryption.

4. **AI-Powered Exploits and Hacking Tools:** Cybercriminals use AI-based tools to perform reconnaissance, identify weak points in a system, and exploit vulnerabilities faster than humans. These tools can discover zero-day vulnerabilities, enabling attackers to infiltrate systems before patches are available. AI also accelerates the process of brute force attacks on passwords by rapidly testing combinations or analyzing user habits to guess credentials.

5. **Deepfakes and Synthetic Identity Fraud:** AI-generated deepfakes—realistic fake videos or audio recordings—are used for impersonation, fraud, or disinformation. Cybercriminals can manipulate deepfake technology to trick individuals, commit fraud, or even blackmail organizations by impersonating high-profile figures. Additionally, AI can generate synthetic identities that combine real and fabricated information, making it harder for financial institutions or security systems to detect fraudulent activities.

6. **AI-Driven Data Poisoning:** AI systems are vulnerable to "data poisoning" attacks, where malicious actors corrupt the datasets used to train AI models. By feeding incorrect or biased data into the training process, cybercriminals can manipulate AI models to make faulty decisions, such as misclassifying malware as benign or overlooking malicious activity.

7. **AI for Reconnaissance and Targeting:** AI systems can sift through massive amounts of publicly available data to build detailed profiles of potential targets. This intelligence can be used to design more effective attacks tailored to specific individuals or organizations, such as business email compromise (BEC) or spear-phishing attacks targeting high-value executives.

AI in Cybersecurity (Defensive Role):

1. **Threat Detection and Response:** AI can help identify and respond to threats faster than traditional methods. AI algorithms analyze vast amounts of data in real-time to detect anomalies, suspicious behavior, or known attack patterns. It can automatically flag or block potential threats before they cause harm.

2. **Behavioral Analysis:** AI is increasingly used for behavioral analysis in cybersecurity. By monitoring user activity, AI systems can identify abnormal patterns that may indicate an attack or insider threat. This helps in detecting threats that might bypass rule-based systems.

3. **Automated Incident Response:** AI can automate certain aspects of incident response, such as isolating infected systems, stopping ongoing attacks, and remediating vulnerabilities. This reduces the time it takes to mitigate damage from cyberattacks and helps organizations recover more quickly.

4. **Predictive Analytics:** AI's predictive capabilities allow security teams to anticipate future attacks by identifying emerging threats based on historical data. This proactive approach helps organizations to prepare for potential risks before they escalate into real attacks.

5. **Vulnerability Management:** AI can help in scanning systems for vulnerabilities more accurately and efficiently than human-led efforts. It can prioritize critical vulnerabilities and recommend patching schedules, allowing organizations to focus on the most significant risks.

6. **Fraud Detection:** In financial services and online transactions, AI is used to detect fraudulent activities by analyzing transaction patterns. AI systems can identify suspicious transactions, account takeovers, and other fraudulent activities with greater precision.

7. **Enhanced Identity and Access Management:** AI-based systems can enhance identity verification processes, including the detection of anomalies in login attempts and multi-factor authentication. AI can detect if a login attempt is legitimate based on factors such as user behavior, location, and device type.

Challenges:

- **AI Arms Race:** As AI becomes more advanced, both cybercriminals and security professionals are engaged in a technological arms race. Criminals are constantly finding new ways to exploit AI, while cybersecurity experts are working to develop countermeasures.

- **False Positives and Bias:** AI systems can generate false positives, overwhelming security teams with alerts that may not be actual threats. Additionally, biased AI models might overlook certain threats or unintentionally prioritize the wrong risks.

- **AI Attacks on AI Systems (Adversarial AI):** AI models themselves are targets. Adversarial attacks manipulate AI models by introducing subtle inputs that cause them to make incorrect decisions, like misidentifying a threat or classifying malicious activity as benign.

CONCLUSION

- Artificial intelligence represents both an opportunity and a challenge in the realm of cybersecurity. On one side, AI enhances the ability to detect, respond to, and prevent cyber threats by automating security processes, identifying patterns, and predicting future attacks. It allows organizations to scale their defenses in ways that were previously impossible and helps mitigate the increasingly sophisticated tactics employed by cybercriminals.

- However, the rise of AI also gives cybercriminals access to unprecedented capabilities, enabling them to launch highly targeted, efficient, and adaptive attacks. AI allows criminals to automate large-scale operations, create personalized phishing schemes, develop intelligent malware, and evade traditional security measures. Moreover, the use of AI in adversarial attacks, deepfakes, and data poisoning adds new layers of complexity to the cybersecurity landscape.
- The challenges posed by AI in cybercrime include the potential for an "AI arms race" between attackers and defenders, the exploitation of AI vulnerabilities, and the lack of skilled professionals who understand both AI and cybersecurity. Moreover, ethical concerns about biased AI systems, adversarial attacks, and the misuse of AI technologies further complicate the situation.
- To combat the growing threats posed by AI-driven cybercrime, organizations must:
- **Adopt AI-based security solutions** that can anticipate and respond to evolving threats in real-time.
- **Invest in the continuous development of AI models** to enhance their robustness and resilience against adversarial attacks.
- **Close the AI skills gap** by training more professionals who can understand and mitigate AI-related threats.
- **Collaborate with regulators** to create frameworks that hold both attackers and defenders accountable in the age of AI-driven crime.
- In the end, the future of cybersecurity will depend on a delicate balance between leveraging AI's potential for defense and mitigating the risks it poses when used for malicious purposes. Organizations must stay ahead of cybercriminals by continuously improving AI security measures and remaining vigilant against emerging AI-driven attack strategies.
