Article Review #2Understanding the Use of AI in Cybercrime

Clarrissa Darden April 6, 2025

Introduction

The article *"Understanding the Use of Artificial Intelligence in Cybercrime"* by Choi, Dearden, and Parti (2024) delves into how criminals exploit artificial intelligence (AI) technologies to carry out cybercrimes. It discusses emerging threats like deepfakes and social engineering in the context of new technologies such as the metaverse. This topic connects to the principles of criminology and sociology by examining how technological advancements can impact crime patterns and societal behaviors.

Research Questions and Hypotheses

The research in this article focuses on understanding how AI contributes to cybercrime, specifically examining the risks posed by deepfakes, social engineering, and AI-generated malware. The study also aims to explore trends in AI-driven crimes and proposes strategies for preventing these criminal activities. The hypotheses are centered on identifying the role AI plays in facilitating these crimes and suggesting preventative measures to address the challenges posed by these technologies.

Research Methods

To address these questions, the authors employ a combination of theoretical frameworks, particularly Routine Activity Theory (RAT) and Cyber-Routine Activities Theory (Cyber-RAT). These frameworks are used to analyze the behavior of cybercriminals who exploit AI technologies and identify the vulnerabilities that make certain individuals or systems more prone to attacks. The research utilizes both qualitative and quantitative methods, including expert

interviews and analyses of AI-driven threats such as large language models (LLM) and AI-based malware. This mixed-method approach provides a thorough examination of the current state of AI-enabled cybercrime.

Data and Analysis

The study provides a comprehensive analysis of how AI is being used to commit cybercrimes, such as creating deepfake images and videos or conducting sophisticated social engineering attacks. The authors gather data through case studies and expert interviews to understand the characteristics of cybercriminals, their motivations, and the factors that make certain targets more vulnerable. By examining these aspects, the authors highlight the growing risks posed by AI and the need for increased cybersecurity awareness and protective measures.

Connection to Course Concepts

This article connects to concepts discussed in criminology and cybersecurity, particularly in understanding how new technologies shape criminal activities. The integration of Routine Activity Theory and Cyber-Routine Activities Theory in the study reflects the sociological and criminological aspects of how opportunities for crime arise and how technological innovations influence these opportunities. This aligns with class discussions on the evolving nature of crime in the digital age and the importance of adapting security measures to new threats.

Marginalized Groups and Their Vulnerabilities

AI-driven cybercrimes, such as deepfakes and social engineering, often disproportionately affect marginalized groups. Individuals from lower socio-economic backgrounds or those with limited access to digital literacy resources are more likely to become victims of these crimes. The article

highlights how these vulnerabilities can be exacerbated by the widespread use of AI, making it harder for marginalized groups to protect themselves. Addressing these issues is crucial to ensure that the risks of AI-driven cybercrime are mitigated across all sectors of society.

Conclusion

The article *"Understanding the Use of Artificial Intelligence in Cybercrime"* contributes valuable insights into the intersection of AI and cybercrime. By examining the use of AI in criminal activities and proposing preventive measures, the study provides a clearer understanding of how technology is shaping the future of cybercrime. The research emphasizes the importance of a multi-disciplinary approach to cybersecurity that integrates technology, policies, and education. Additionally, the article underscores the need for proactive measures to protect vulnerable groups from AI-driven cybercrimes. Overall, this study serves as an important resource for understanding the risks posed by AI in the context of cybercrime and provides a foundation for further research and policy development.

References

Choi, S., Dearden, T., & Parti, K. (2024). Understanding the use of artificial intelligence in cybercrime. *International Journal of Cybersecurity Intelligence and Cybercrime, 7*(2), 1-3. Understanding the Use of Artificial Intelligence in Cybercrime