Berline Najacque

Old Dominion University

CYSE 201s

Article Review 1

Bora Aslan

February 14, 2025

Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures

Introduction

Artificial Intelligence is a leading technology which studies the ways how smart machines and intelligent programs can creatively solve complex problems. At the same time, AI has enormous potential to promote innovation and enhance efficiencies across many different industries. The article "Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures" examines how people use AI to commit cybercrime.

The Principles of the Social Sciences

The article outlines several social science principles, including relativism, is examines the interactions and effects of many aspects of society and technological developments. Objectivity understanding AI cybercrime using facts and evidence. Parsimony demonstrated the solutions proposed to mitigate cyber threats, empiricism reflected in the study's reliance on observed and experimental data and ethical neutrality is a standard in the research process, and the analysis of cause-and-effect relationships between AI use and cybercriminal activities explains determinism.

Research Hypotheses

The study looks at how different countermeasures are effective, how artificial intelligence technologies are used to support cybercrime, and the developing pattern in AI cyberattacks. According to the article, some AI cyber-attacks are more sophisticated and challenging to detect. (Shetty,2024).

Types of Research Methods Used

The study used quantitative and qualitative methods to examine the role of artificial intelligence cybercrime activities. The quantitative analysis provided an understanding of AI-generated prompts and online conversation, while the qualitative reported the legal, technical, and policy (Shetty,2024).

Data and Analysis

The study highlights that they used Onion Router to gain access and collect information on AI-generated prompts that are utilized for malicious attacks. Include details about the software and screenshots of the prompts from different platforms like Reddit and FlowGPT.

Concepts from PowerPoint Presentations

The article highlights cybersecurity's importance and social engineering's role in cyberattacks. It also discusses the ethical consequences of AI in cybersecurity and the psychological impacts of cybercrime on victims.

Challenges, Concerns, and Contributions of Marginalized Groups

The article emphasizes marginalized groups' challenges and concerns when the communities attempt to use certain cybersecurity technologies they cannot. Moreover, the study emphasizes the role of AI-enabled cyber risks in affecting social groups. (Shetty,2024).

Contributions to Society

The studies contribute to society by providing excellent knowledge of AI cybercrime and best practice strategies for prevention. They emphasize how crucial it is to educate people about cybersecurity, collaborate across industries, and create policies that safeguard everyone in society.

Conclusion

Therefore, the study uses several methods to investigate the connection between AI and cybercrime. It helps us understand how complicated AI-driven cybercrime is, the problem that marginalized groups face, and how important it is to teach people about cybersecurity work to make the world safer.

References

Shetty, S., Choi, K., & Park, I. (2024). Investigating the intersection of AI and cybercrime: risks, trends, and countermeasures. *International Journal of Cybersecurity Intelligence and Cybercrime*, *7*(2). https://doi.org/10.52306/2578-3289.1187