Samuel Woodruff

CYSE 201S

Professor Yalpi

10/2/2024

Article Review #1: Understanding the Use of Artificial Intelligence in Cybercrime

Introduction

The article '*Understanding the Use of Artificial Intelligence in Cybercrime*', written by authors Dr. Sinyong Choi, Dr. Thomas Dearden, and Dr. Katalin Parti dives into the vastly understudied frontier of the use of artificial intelligence in cybercrime. Artificial Intelligence has taken massive leaps over the past decade and the full ramifications of AI, especially in regards to cybercrime, is still unknown. The authors' purpose in writing the article is to bring attention to the potential harm AI may bring to cyberspace and how professionals can develop potential risk identification, mitigation, and prevention methods.

Study #1 Hypothesis, Research, and Findings

Study One questioned the overall cybersecurity challenges the healthcare sector faces and how the field may be better secured through education, awareness, and better practices. The first study used Routine Activity Theory to analyze cybercrime case studies as well as identify potential motivators, targets, and flaws in regards to a cybersecurity guardian. At the conclusion of the study, it was found that there was a, "...need for a proactive, multi-layered approach to

cybersecurity in the healthcare industry, emphasizing the integration of the VIVA components into these frameworks to enhance resilience against cyber threats" (Choi, Dearden, Parti, p. 2, 2024).

Study #2 Hypothesis, Research, and Findings

Study two raised the question of how the realms of AI and cybercrime are interconnected and identifies potential risks and [possible preventative steps. The study utilized regular Routine Activity Theory as well as Cyber-Routine Activity Theory to identify motivators, vulnerabilities in targets, and lack of guardianship. The study was able to find through both qualitative and quantitative data analysis that large language models present a great cybersecurity threat.

Study #3 Hypothesis, Research, and Findings

The third and final study of the article used the Integrated Model of Cybercrime Dynamics to identify individual, environmental, and behavioral factors in regards to cybercrime. Essentially, the third study focused on the use of the IMCD to better understand these factors to facilitate better planning, policies, and education.

Relations to Core Concepts, Social Science Principles, and Marginalized Groups

This article is full of relations to the course's core concepts as well as social science principles. In regards to social science principles, the article uses multiple principles ranging from utilizing empirical research through experimentation, using data collection following testing, as well as both quantitative and qualitative data analysis. The article also explores some of the core concepts of CYSE 201S as well. Some concepts that're explored are motivators for committing

cybercrime, the concept of determinism as it relates to cybersecurity, understanding proper cyber hygiene, and use of the scientific method to better secure cyberspace. The use of AI in cybercrime has massive implications on marginalized groups. For instance, deepfakes may be used to target marginalized groups like minorities and women to further stigmas. Likewise, AI cyberattacks can be used to target those less fortunate through phishing and other scams.

Conclusion

As a whole, the article delves deep into the rapidly developing topic of AI use in cybercrime. The article excellently brings attention to the possible threats that AI poses in regards to cybercrime even in more niche sectors of society like healthcare. The studies performed help to better understand the driving forces behind AI use in cybercrime, possible mitigation and prevention strategies, and ways forward. Overall, the article covers an extremely understudied topic and brings much-needed attention to this rapidly evolving challenge.

Works Cited

Choi, S. , Dearden, T. & Parti, K. (2024). Understanding the Use of Artificial Intelligence in Cybercrime . International Journal of Cybersecurity Intelligence & Cybercrime, 7(2), - . DOI: https://doi.org/10.52306/ 2578-3289.1185 Available at: https://vc.bridgew.edu/ijcic/vol7/iss2/1