Article Review #2: The Analysis of AI and Cybercrime in the Modern Age

Student Name: Cameron Kim

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Diwakar Yalpi

Date: 14 April 2026

Introduction

This article review examines how AI enables cybercrime and shows how much the social sciences can create an effective response to cyber attacks.

Relation to the Principles of Social Sciences

This article highlights the ever growing correlation between artificial intelligence and cybercrime. As a core piece of the social sciences, this topic focuses not on just the technology itself, but about how people use the technology and how it affects society. The authors of the article used "the Cyber Routine Activities perspective as the theoretical foundation" (Shetty 29) to show how people's online behavior can affect and expose users to risks. This proves how a user's behavior goes hand in hand with technology.

Hypothesis

This article asks multiple questions: How is AI used in cybercrimes? Are there any patterns showing through the cracks as AI gets better? What can we do as a society to fight back against these crimes?

Types of Research Methods

The authors used a qualitative researching method instead of a quantitative method. They focused on understanding current circumstances and previous attacks and analyzed patterns. Using already conducted research, they got real world insight on the matter. This helped them realize how AI is being used in these cyber attacks.

Types of Data

The authors of the article used multiple types of data. They got primary data from personally conducted interviews of cybersecurity experts and got secondary data by citing information from books and academic articles.

Relation to the Course

This topic relates to the topics we have been working on in the weekly modules. This topic talks heavily about online safety and ethical usage of technology like AI and how the social sciences affect the defense and response to attacks.

Relation to Real Life

The authors of this article make the point that people with limited online access and knowledge are often hit hardest by AI-driven attacks. Bias in AI systems can also hurt disadvantaged areas more than other communities. This article addresses these issues with the intention of educating readers about protecting everybody, including those most vulnerable to AI led attacks,

Contributions of this Study to Society

This study raises awareness for a threat that is still emerging and constantly evolving. The authors state the problem and possible solutions for these problems, such as better cybersecurity education and policies, and collaboration with governments to increase defense. This article is a good insight on how social science and technology can collaborate to make society safer and better protect future generations.

Conclusion

This article emphasizes how AI is changing and evolving cybercrime and how the social sciences are an important piece in the understanding of this new wave of attacks. The authors suggest an increase of government involvement, especially for more vulnerable communities. Technology and society are more deeply connected than ever and should continue to be in order to stay safe in this developing modern age.

Works Cited

Shetty, Sanaika, Kyung-Shick Choi, and Insun Park. “Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures.” *International Journal of Cybersecurity Intelligence and Cybercrime*, vol. 7, no. 2, 2024, pp. 28-53. Bridgewater State University, https://vc.bridgew.edu/vol7/iss2/3/.