Nicholas Morton
Date: September 29, 2024

Article Review #1: Investigating the Intersection of AI and Cybercrime

Introduction

The article "Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures" by Shetty, Choi, and Park (2024) shows how Artificial Intelligence is now starting to be used in cybercrime. It was published in the International Journal of Cybersecurity Intelligence & Cybercrime and it studies the threats posed by AI and how to solve them. Since AI tools are easily accessible, AI is now being used by cybercriminals and is making this a critical area of research. (Shetty and others, 2024)

Relevance to Social Sciences

Cybercrime driven by AI relates to the principles of social sciences, particularly in Criminology and Sociology. The article shows how human behavior and social structures can be exploited by cybercriminals through AI. The authors of the article uses Choi's (2008) Cyber Routine Activities Theory (Cyber-RAT) to show how daily online activities, or "routines," can make individuals vulnerable to cyber threats (Shetty and others, 2024). This framework shows the meeting of technology and human behavior.

Research Questions and Hypotheses

The article addresses three research questions, for example:

1. How is malicious AI information spread across the dark web and now the clear web
2. What roles does the media play in the spread of AI-driven cybercrime
3. How can practices reduce AI-related cyber threats?

The authors of the article hypothesize that AI's availability to the public makes it very easy for criminals to target individuals, specifically those who are not good on the web. (Shetty and others, 2024)

Research Methods

In the article, the authors use both quantitative and qualitative and quantitative methods. They used the TOR browser to collect quantitative data from forums on the dark web. They gathered 102 AI-generated malicious prompts which were used for phishing, malware, and ransomware. They also interviewed six cybersecurity experts to get more information of the topic. (Shetty and others, 2024)

Data and Analysis

The quantitative data revealed that AI-generated malicious activities can be found on dark web forums. With the use of tools like ChatGPT, are used to create harmful software or can manipulate users into cyber scams. They also used interviews to bring context to the quantitative data and emphasized the evolution of cybercrime because of AI (Shetty and others, 2024)

Connections to Class Concepts

The article uses several principles that we talked about in class. For example, the principle of relativism is present in how changes in one societal system can lead to changes in others, such as criminal

justice and social behavior. Empiricism is also present because they examined real-world data from the dark web forums posted.

Conclusion

In conclusion, the study contributes to the understanding of cybercrime driven by AI. It talks a lot about the importance of being safe online to prevent victimization. Connecting theory to solutions, the article also offers how to address AI role in cyber threats and how to solve them. (Shetty and others, 2024)

References

Shetty, S., Choi, K., & Park, I. (2024). Investigating the intersection of AI and cybercrime: Risks, trends, and countermeasures. *International Journal of Cybersecurity Intelligence & Cybercrime, 7*(2), 28-53. https://vc.bridgew.edu/ijcic/vol7/iss2/3