Carter Wood

Article Review #2

CYSE 201S

10 April 2025

The Dark Side of Intelligence: A Review of AI and Cybercrime in the Digital Age

This article reviews how AI is enabling cybercrime and emphasizes the need for social science–based strategies to understand risks and shape effective responses.

Relating to the principles of social sciences

This article explores the growing connection between artificial intelligence (AI) and cybercrime, a topic that fits right into the core of social sciences. It's not just about technology; it's about how people use technology, how it affects society, and how we respond as a community. The authors use a theory called Cyber Routine Activities Theory to show how our regular online behavior can expose us to new risks. This really highlights how technology and human behavior go hand in hand, a key principle in the social sciences.

Hypothesis

The article doesn't lay out formal hypotheses, but it does ask some really important questions: How are criminals using AI to commit cybercrimes? What trends are we seeing as this technology evolves? What can we do through policy, education, or technology to prevent and fight back against these crimes?

Types of research methods

The authors used a qualitative research approach, meaning they focused on understanding experiences and patterns instead of crunching numbers. They did a concept review of existing research and also interviewed cybersecurity professionals to get real-world insights. This gave them a broader view of how AI is being misused and what steps we might take to stay ahead of cybercriminals.

Types of data

The study used two types of data: Secondary data from books, academic articles, and reports; and Primary data from expert interviews. They used a concept analysis to pull out common ideas and trends from all this information, which helped shape their recommendations on how to respond to AI-powered cybercrime.

Concepts relating to the modules

This topic is related to the topics discussed in the modules. This relates by talking about digital safety, ethical tech use, and how social structure can respond to specific changes. The use of theory to explain cybercrime is a great example of how social science concepts can help us understand and manage real-world issues involving technology.

Topic relating to challenges

The article points out that people with limited digital literacy or fewer resources are often the ones hit hardest by AI-driven cybercrime. It also touches on how bias in AI systems can hurt marginalized communities even more. So, addressing these issues isn't just about stopping crime so it's about protecting everyone fairly, especially those who might be more vulnerable.

Contributions of the studies to society

In the big picture, this study helps raise awareness about a threat that's still emerging. It doesn't just point out the problem so it also offers solutions, like better cybersecurity education, smarter policies, and collaboration across tech, law, and government. It's a great example of how social science and tech can come together to make society safer and more prepared for the future.

Conclusion

This study highlights how artificial intelligence is reshaping cybercrime and why a social science approach is crucial to understanding and responding to it. The authors call for better education, stronger policies, and inclusive protections, especially for vulnerable communities. It's a reminder that technology and society are deeply connected, and both must evolve together to stay safe in the digital 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. 109–127. Bridgewater State University, https://vc.bridgew.edu/ijcic/vol7/iss2/5/.