Keith Bartlett

02/14/2025

# Article Review #1

# AI-Empowered Cybercrime:

https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1187&context=ijcic

## Research Questions and Methods

This study investigates the intersection of artificial intelligence and cybercrime, focusing on three main research questions:

1. How is malicious AI-related information distributed between the dark and clear web? (Shetty et al., 2024)
2. What role does media play in spreading AI-facilitated cybercrime? (Shetty et al., 2024)
3. How can individual cyber hygiene practices be improved to reduce AI-based threats? (Shetty et al., 2024)

The researchers used a mixed-methods approach, combining quantitative and qualitative techniques.

## Data Collection and Analysis

Quantitatively, they collected and analyzed 102 malicious AI prompts from various online forums on both the clear and dark web. (Shetty et al., 2024) Qualitatively, they conducted semi-structured interviews with six experts in cybercrime, cybersecurity, and criminal justice. The quantitative data analysis involved categorizing AI tools, content types, and forums where malicious prompts were found. The qualitative data from expert interviews underwent thematic analysis to identify recurring themes and insights. (Shetty et al., 2024)

## Relevance to Marginalized Groups

While the study does not explicitly focus on marginalized groups, it addresses broader societal concerns that can affect vulnerable populations. The research highlights how AI-facilitated cybercrime can worsen existing inequalities, potentially leaving marginalized communities more susceptible to cyber threats due to limited resources or awareness. (Shetty et al., 2024)

## Contributions to Society

The study makes several contributions to society:

1. It provides a comprehensive understanding of AI's role in cybercrime, bridging the gap between clear and dark web activities.
2. It emphasizes the need for improved cyber awareness education.
3. It suggests developing AI-driven solutions to combat malicious content, potentially enhancing cybersecurity measures.
4. It advocates for more specific cybercrime legislation to address emerging AI-related threats.
5. It highlights the importance of ethical considerations in AI development and deployment.

## Applications of Principles

The study applies several principles of social science to cybersecurity research. It emphasizes empiricism by collecting and analyzing quantitative data on malicious AI prompts. The research demonstrates objectivity by examining both dark and clear web content without bias. Parsimony is evident in the focused research questions and hypotheses. The study also exhibits determinism by exploring how AI technologies influence cybercriminal behaviors. Additionally, it employs skepticism by critically examining expert opinions and considering alternative explanations for cybercrime trends. Overall, the research exemplifies how social science principles can be applied to study complex technological phenomena like AI-facilitated cybercrime.

## Relations to Presentations

The PowerPoint presentations and the article both emphasize the importance of understanding human factors in cybersecurity. The presentations discuss psychological theories explaining cyber offending, such as cognitive and behavioral theories, which align with the article's focus on the psychological aspects of AI-facilitated cybercrime. They also highlight the role of individual motivations and behaviors in cybersecurity incidents. The presentations' discussion of victim behaviors and risk factors relates to the article's examination of how online lifestyles and routines can increase vulnerability to AI-driven cyber threats. Additionally, both emphasize the need for improved cyber awareness and education to mitigate risks, which is a key recommendation in the article for addressing AI-related cybersecurity challenges.

## Conclusion

By shedding light on the complex dynamics of AI-facilitated cybercrime, this research contributes to the development of more effective strategies for cybercrime prevention. It underscores the need for collaborative efforts among policymakers, educators, and cybersecurity experts to create robust frameworks for safeguarding digital environments in an increasingly AI-driven world.

Works Cited

Shetty, S., Choi, K.-S., & Park, I. (2024). *Investigating the intersection of AI and Cybercrime*. Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1187&context=ijcic