### Article Review # 1

Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures

### Introduction

The article "Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures" by Shetty, Choi, and Park (2024) explores the growing influence of AI in both cybersecurity and cybercrime. While AI can strengthen digital defenses, criminals are also leveraging it for illegal activities. This review breaks down the article’s key points, its connection to social science, the findings.

### How It Relates to Social Science

This study examines human interactions with technology and how bad actors take advantage of them. Using Routine Activities Theory (RAT) and Cyber RAT, it explains how criminals find and exploit victims online. It also highlights the importance of cybersecurity awareness and ways to safeguard personal information.

### Research Questions

The study focuses on three key questions:

1. How do criminals distribute AI-based cybercrime methods on the dark web and mainstream internet?
2. What influence does the media have on AI-driven cybercrime?
3. What measures can individuals take to protect themselves from AI-related cyber risks?

### Research Methods

To explore these questions, the researchers analyzed discussions in online forums to understand how AI is being misused by cybercriminals. They also conducted interviews with cybersecurity and criminal justice experts to gain professional insights into these trends. This combination of data and expert opinion helped create a more complete picture of the problem.

Findings and Analysis

The study identified 102 instances of AI-generated cyber threats appearing in both dark web and public forums. These included phishing schemes, malware, and fraud. AI tools like ChatGPT and WormGPT were commonly mentioned in these activities. Experts in the study emphasized that as AI continues to evolve, criminals will develop new ways to exploit it. The study suggests that increasing awareness and implementing stronger security measures are crucial in countering these threats.

### Connection to Course Concepts

The article relates to cybersecurity, digital ethics, and online safety. It applies criminology theories like RAT to explain how cybercriminals operate and highlights the importance of digital literacy in preventing online scams and misinformation.

### Impact on Marginalized Communities

AI-driven cybercrime disproportionately affects marginalized groups, such as low-income individuals, older adults, and women. These communities are often the targets of financial fraud and deepfake exploitation. The study stresses the importance of providing cybersecurity education and implementing policies to better protect vulnerable populations.

### Why It Matters

This research highlights how AI is reshaping cybercrime and why people need to be aware of these changes. Understanding these risks helps individuals and organizations take proactive measures to protect themselves. The study calls for stronger AI regulations, improved cybersecurity education, and greater public awareness to prevent AI misuse.

### Conclusion

Shetty, Choi, and Park (2024) present a thorough analysis of how AI is influencing cybercrime. Their research combines data analysis with expert opinions to provide a well-rounded perspective on this issue. As AI technology continues to grow, staying informed and improving cybersecurity practices will be crucial in reducing cyber threats.

### 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://doi.org/10.52306/2578-3289.1187>