# Article review #1: A Review of the Dark Side of AI in Cybercrime

Daniel BrzezinskiRockwell

20 February 2025

Prof. Yalpi

CYSE 201S

**Intro:**

Regarding recent groundbreaking innovations or applications that have changed everyone's lives in some aspect has been the mainstream introduction of "Artificial Intelligence," aka A.I. There are many distinct types of artificial intelligence that are used in a myriad of data collection, pattern recognition, and deep learning which has been adopted the most recently. The article *Investigating the Intersection of A.I. and Cybercrime: Risks, Trends, and Countermeasures* covers how this has occurred in recent years and the drastic countermeasures taken to combat this new threat. Starting with the thesis statement, a review of how the paper addresses issues presented and a basic lookover of how the authors constructed their article.

**Structure analysis:**

The article's structure is well constructed with the intro establishing a base knowledge so that the reader will understand the article's terms and line of reasoning. In the intro, the thesis statement is brought forward into its paragraph to draw attention, followed by a description of how the researchers plan to study the topic. The method used to study the data acquired was thematic analysis for literature and interviewing professionals in cyber security and cybercrime. (Shetty pg. 29) Thematic analysis is an analysis of qualitative data to identify recurring patterns and themes in data to establish trends and interrupt what the data is showing.

**Thesis and research questions:**

The thesis gives a straightforward issue that the article will address with the data collected, "this study examines the intricate relationship between AI and cybercrime, particularly focusing on how AI can be exploited for malicious purposes." (pg. 29) The researchers later describe how A.I. apps were given malicious prompts to help generate programs that could later be used in a form of cybercrime. They show that the cost of entry into the practice of committing these crimes has nearly disappeared as anyone with access to these tools and a base knowledge could utilize them.

The article also gives the reader recommendations on how to be better prepared for these types of crimes and having better cyber hygiene, "...the responsibility for capable guardianship falls upon individuals' cyber hygiene and activities on the internet or related technologies." (Shetty pg. 32) It goes on to say that personal cyber is the most effective way to combat emerging threats online. The researchers also used the tool that enables cybercrime in the first place, A.I., as a countermeasure to counteract the crimes committed. Collaboration between companies and governmental policies will have to be made for a more comprehensive effort.

**Conclusion:**

After careful examination of the article selected and review of how the authors conducted their research, applied their methodology in examining the data they collected, and the conclusion they made with recommendations that would help the reader, the article is well made and comprehensive. As society adopts A.I. in greater capacities in everyday life, more significant consideration of individual safety must be made and taught. Like the introduction of the internet and its rapid growth in every part of society, the true magnitude of what has been brought is yet to be had.

# References:

Shetty, S., Choi, K.-S., & Park, I. (2024). Investigating the intersection of AI and cybercrime: risks, trends, and countermeasures. *International Journal of Cybersecurity Intelligence &amp; Cybercrime*, *7*(2). https://doi.org/10.52306/2578-3289.1187