Hector Phan

4/03/2025

CYSE 201S

Article Review #2

Acknowledging Artificial Intelligence's Involvement in Cybercrime

BLUF: Sinyong Choi, Thomas Dearden, and Katalin Parti's article "Understanding the Use of Artificial Intelligence in Cybercrime" explores how AI being used to help combat cybercrime. The authors explains how artificial intelligence is used to regulate criminal activities such as malware development, phishing, and data breaches, improving the speed and challenges of identifying cybercrime. The research also highlights that AI has two viewpoints: it can serve as a weapon for criminals and a solution for cybersecurity professionals. A broad approach to manage cybersecurity and upgrade security measures which is necessary due to the increasing risk of AI attacks.

Introduction

The connection between artificial intelligence and cybercrime has been studied in the article "Understanding the Use of AI in Cybercrime by Sinyong Choi, Thomas Dearden, and Katalin Parti”. The authors focus on the impact of AI technologies in the changing of digital crime. The assessment will focus on the article's connection to the social science principles, the research questions and methods of the study, the different types of data and analysis used, the article's relevance to the disadvantaged groups, and its social contributions.

Relation to the Principles of Social Sciences

The study links the building blocks of social sciences through an exploration of how technological progress, in this case artificial intelligence, influences human behavior and social organization.

The study investigates how AI is impacting power dynamics, digital security, and social order, as well as how it is reshaping the pillars of cybercrime. The primary goal of the social sciences, specifically sociology and criminology, is to understand how society changes. This piece illustrates how crime, law enforcement performance, and public safety are influenced by modern technologies.

Research Questions and Hypotheses

The article's main objectives focus on how artificial intelligence can help cybercrime. The study focuses on how hackers use AI to create their crimes more complicated and broader. The authors have probably predicted that the use of AI in cybercrime makes detection and avoidance more challenging. The article also looks at whether AI can help cybercriminals grow and alter their tactics.

Research Methods

A combination of qualitative and quantitative research techniques was used by the researchers. These typically require a thorough examination of the results of research on AI, cybercrime, and their involvement. To understand the actual uses of artificial intelligence in criminal behavior, the authors looked at case studies, cybercrime trends, and possibly the viewpoints of cybersecurity experts. AI-driven crime's technological and social aspects can be thoroughly investigated due to the mixed-method approach.

Types of Data and Analysis

The primary source of data that involves the article is secondary sources, including research publications, case studies, and reports on the use of AI in cybercrime. The authors study patterns of AI-enabled criminal activity, focusing on common methods such as automated phishing, deepfakes, and AI-assisted hacking tools. The analysis possibly includes looking into previous trends in cybercrime and comparing how well or how poorly security measures have worked to prevent these AI threats. The essay focuses on how AI makes cyber criminals more skilled, leading to the need for advanced security systems.

Connection to PowerPoint Concepts

The article relates to several topics that often appear in the classes' PowerPoint presentations, such as the creation of cybercrime, the ethical challenges created by new technology, and the increasing role that artificial intelligence in modern security issues. The article's focus on AI's effects on cybersecurity and crime prevention directly relates to important issues, which include the moral uses of AI, the role of technology in criminal actions, and finding a balance between digital security and privacy. It helps the fact that to prevent new technologies from making known vulnerabilities more severe, laws and procedures must constantly evolve.

Impact on Marginalized Groups

Individuals with low incomes and communities with limited access to advanced technology and security measures fall under those who are disproportionately impacted using AI in cybercrime. Due to their lack of the finances or knowledge to protect themselves, individuals like them are more vulnerable to identity theft, online fraud, and other artificial intelligence cybercrimes. Since disadvantaged communities usually face greater challenges when seeking protection or legal solutions, the gap in technology may increase the impact of these crimes. The article brings awareness to these problems and warns individuals to think about vulnerable communities into consideration when managing AI.

Contributions to Society

By improving the knowledge of how AI can influence cybercrime and the challenges it brings for cybersecurity, the study can help society by teaching others how to avoid these issues. It explains how important it is to update the legal structures to keep up with the changes in technology and the need for more advanced security measures. By identifying the potential negative effects of AI on cybercrime, the article also supports the advances of cybersecurity education, better protections, and more public awareness of online dangers. To be able to create a safer digital environment, the research shows the value of community adjustment to adapt to these new threats.

Conclusion

To summarize the topic, understanding the use of artificial intelligence in Cybercrime can offer important information on how AI can be used in criminal activity. To help lower the dangers that AI brings to cybercrime, studies can show the value of updated rules and regulations, safety measures, and educational programs. It also shows the need of a complete approach to resolve the challenges by looking at the social, ethical, and technical aspects of AI's involvement in cybercrime. Due to constantly changing technologies, it also brings awareness to the vulnerabilities of those who are not knowledgeable and encourage more efforts to protect them.

References:

Sinyong, C., Thomas, D., & Katalin, P. (2024). Understanding the Use of Artificial Intelligence in Cybercrime. In. Center for Cybercrime Investigation & Cybersecurity.