Article Review #1 - The Onset of AI as Related to Cybercrime and Society

Collin Sloan

UIN - 01267943

CYSE 201S: Cyber Security and the Social Sciences

Diwakar Yalpi

February 16, 2025

Relation to Social Sciences

The topic of Artificial Intelligence (AI) in conjunction with cybercrime relates to social science fields in various ways to various societal groups. The internet allows for this AI chatbot, such as Chat GPT, to think for human beings through informational based speculation and research. AI can be utilized by potential criminals to victimize multiple people simultaneously through technological means. Social sciences such as Sociology or Psychology, encompass the studies of various aspects of human motivators, intelligence and behaviors. This topic of AI in cybercrime could truly allow for the planned domain to attack the victim (s) through computer algorithms.

Research Questions

Through research questions, AI can outline the markers to distribute information over the internet with possible intent to do harm. The media outlets show that AI is reaching a larger audience which sensationalizes cybercriminal activities. The questionable data needs to be kept clean so practices need to be in place to stay ahead of underlying dangers of AI chatbot usage.

Research Methods

The research methods included " Using the Cyber Routine Activities perspective as the theoretical foundation, we conducted interviews with academic and practical experts in cybercrime, cyber-security, and criminal justice" (Shetty et al., 2024). These methods were further extended to show "Our quantitative research provided in-sights into AI-generated prompts and the discussions surrounding these prompts on online forums, while our qualitative research informed us on the legal, technical, and policy solutions needed to address the findings from the quantitative research." (Shetty et al., 2024).

Data Analysis

There were types of data and analyses that show responses to the prompts were collected from online group polling. The data was presented "Specifically, we identified eight distinct forums that served as platforms for AI-generated prompts: FlowGPT, Respostas Ocultas, Reddit, Dread, Legal RC, Hidden Answers, Dark Net Army, and YouTube." (Shetty et al., 2024) in a clear and easily readable format. Further analysis of data was conducted as "In conceptualizing and analyzing the interview questions, we apply Choi's (2008) Cyber RAT as our framework. The Cyber RAT framework extended the traditional Routine Activities Theory to better explain computer crime victimization by underscoring that, in the digital age…" (Shetty et al., 2024).

Powerpoint Information in Relation to the Article

The content concepts from the PowerPoint presentations relate to this article through various aspects of social science lessons. Social science research methods used included surveys that were utilized to gain insight into human behaviors as related to AI and cybercrime. Individuals were polled in order to provide information as requested. Social science cyber research may have a polling group that is not indicative of societal norms thus tampering results.

The relationship between the social science principles and the article shows the true connection of AI data to cybercrime parameters keeping the focus simple and applicable. The principle of Relativism organizes the AI data in a format for the need of the cybercriminal for real-time purposes. Additionally, Societal Systems are relevant to this topic due to the connection of various disciplines of hacking opportunities to AI data in the mind of the possible cybercriminal. Also, the principle of Parsimony is clear in this article as AI presents the information as simply as possible then the intent of the usage of the information fuels cybercrime motivators.

Relation to Marginalized Groups

This topic relates to challenges, concerns and contributions of marginalized groups in multiple ways. Marginalized groups can relate to cybercrime tendencies using AI as being marked possible targeting efforts or even drawn to commit the cybercrime. Examples of these group dynamics include people that are different racially. financially or socially thus all leading back to social science studies.

Concerns of these marginalized groups primarily stem from equal representation or validating a concern through AI and cybercrime. Examples of these acts involve a person holding a grievance to the health insurance carrier looking to possibly create a cybercrime or a specific racial group looking to gain equal treatment could result in cyber criminal activity using AI chatbots. There are so many different marginal groups that could have their own motivation to utilize this rapidly increasing availability of AI information with possible malicious intent.

Overall Contributions to Society

The concept of AI as related to cybercrime contributes to society in a two fold manner. The first fold provides information to the possible cybercriminal to prepare to possibly commit the cybercrime. The next fold blindly provides information to create groups of unknowing victims of various size lots. It is through this feature of survey group dynamics that truly show

how groups can be targeted silently. AI and cybercrime when together manifest a unique yet dangerous relationship.

Conclusion

Conclusions can be drawn after the research methods and data analyses were completed to the testing group. Conceptually, the article contributes to the social science studies of AI and societal groups with the heavy usage of AI technology with the possible malicious intent to facilitate cybercrime. The AI component has shown a connection to cybercrime through the actions over the internet that possibly victimize various groups of people without warning. The data collected from the polling group was analyzed on both quantitative and qualitative methods to gain full understanding of the power of AI with respect to cybercrime.

Source

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), - . DOI: https://doi.org/10.52306/2578-3289.1187 Available at: https://vc.bridgew.edu/ijcic/vol7/iss2/3 Copyright © 2024 Sanaika Shetty, Kyung-Shick Choi, and Insun Park

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

Title of Article - **Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures**