Understanding the Use of Artificial Intelligence in Cybercrime Review

CJ McDonald

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity as a Social Science

Dr. Leigh Armistead

October 8, 2023

How does the topic relate to social science principles? (3 or more)

The article maintains a relatively objective tone throughout, presenting information about the impact of technology on crime without overt bias. It instead relies on research findings and expert opinions to support its claims, promoting objectivity in the presentation of information.

The article also discusses how technology, specifically artificial intelligence, is changing the crime landscape. It acknowledges that criminals adapt and develop new illegal activities. This recognition of changing norms and behaviors in response to technology aligns with the idea of relativism.

Lastly, the article indirectly touches on determinism by exploring the role of technology in criminal activities. It suggests that artificial intelligence enables offenders to commit crimes more effectively, hinting that technological determinism plays a role in shaping criminal behavior in the digital age.

In the end, the article relates to various social science principles such as objectivity, relativism, and determinism.

What are the research questions and hypotheses?

The article doesn't explicitly state the research questions and hypotheses for the two studies, but educated inferences could be made.

For the first study, some research questions could be:

- What are the motivations behind interpersonal cybercrimes, including financial gain and sexual gratification?
- How do the routine activities theory and Eysenck's theory of criminality explain offender characteristics and target vulnerabilities to deepfakes in the metaverse?

Some inferred hypotheses for Study 1 can be:

- Financial gain and sexual gratification are primary motivations for interpersonal cybercrimes in the metaverse.
- Routine activities theory and Eysenck's theory of criminality can help explain specific offender characteristics and target vulnerabilities related to deepfake-related crimes.

For the second study, some research questions could be:

- How can GPT-4 large language modeling be used to simulate target responses to social engineering attacks?
- What are the vulnerabilities of individuals to social engineering attacks?
- How do personality traits, as categorized by the Big Five Personality traits model, influence susceptibility to social engineering attacks?

The inferred hypotheses for the second study:

- GPT-4 LLM can effectively simulate target responses to social engineering attacks.
- Certain personality traits, such as high agreeableness, low conscientiousness, and high neuroticism, are associated with a higher susceptibility to social engineering attacks.

What type of research methods are used?

The first study in the article used a qualitative research method. Qualitative research primarily involves the collection and analysis of non-numerical data. This includes text, interviews, observations, or narratives. Those examples included are to help understand underlying meanings, patterns, and interpretations of a phenomenon.

In contrast, the second study in the article used a quantitative method of research, more specifically, a computational research method. Computational methods involve the use of computer algorithms and numerical data to analyze and model various aspects of a research question. It often includes techniques such as statistical analysis, machine learning, simulations, and data mining. All of those techniques are quantitative, focusing on numerical data, patterns, and statistical relationships.

What types of data and analysis are done?

The first study collected data by conducting eight semi-structured interviews with policy, academic, and industry experts in South Korea. To analyze the data, they did a thematic analysis to identify themes in the expert testimonies on the topics of deepfake crimes in the metaverse.

The second study utilized the GPT-4 large language model to simulate target responses to social engineering attacks, such as phishing attacks. The analyzed data was generated by GPT-4 to assess target vulnerabilities based on personality traits.

How does this article relate to concepts from class? (4 or more)

One of the concepts in class this article relates to is victimization. In class, we learned that there is a psychological role victims play in cybersecurity incidents. Also both in class and in the article, the big five personality traits that increase the risk of becoming a victim are mentioned, an example being neuroticism.

Another class concept this article mentions is social science, specifically, criminology. Criminology refers to the study of crime, criminals, and society's response to them. The relation the article shares is its study of what's motivating criminals to offend, like other criminologists. The motives in the article were more focused on financial gain or sexual gratification, but in class, we discussed more motives such as political reasons and revenge.

A third class concept the article mentions is social engineering attacks. Social engineering is a set of manipulative techniques used to exploit or trick individuals into revealing sensitive information, providing unauthorized access, or performing actions that compromise security. These types of cyber-attacks rely on deception and manipulation rather than technical exploits. The example of social engineering we discussed in class and that's also used in the article is phishing attacks.

Lastly, a fourth concept we discussed in class that relates to the article is the social science principles discussed earlier in the review. The article discussed many social science elements such as relativism, objectivity, skepticism, and determinism. These elements, along with parsimony and ethical neutrality, were all discussed early in the CYSE 201S course.

What are the overall societal contributions of the study? (2 or more)

Study 1 highlights the rising threat of deepfake-related interpersonal crime in the metaverse. It also suggests the need for criminal procedures, police enforcement, and psychological healing programs for victims. Its societal contribution is to raise awareness about this emerging form of cybercrime and propose preventive measures.

Study 2 contributes to the field of cybersecurity by identifying personality traits associated with susceptibility to social engineering attacks. This information can inform the design of more effective cybersecurity systems, potentially offering additional safeguards to individuals with high-risk personality traits.

Both studies provide valuable insights into the intersection of technology and crime, with potential implications for law enforcement, cybersecurity, and criminological research.

References

Dearden, K., & Choi, T. (2023). Understanding the Use of Artificial Intelligence in Cybercrime. *International Journal of Cybersecurity Intelligence &*, *6*(2). https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1170&context=ijcic