Parti et al. (2023). *International Journal of Cybersecurity Intelligence and Cybercrime, 6*(2), 1-2.

Understanding the Use of Artificial Intelligence in Cybercrime

Katalin Parti*, Ph.D., Virginia Tech, U.S.A.
Thomas Dearden, Ph.D., Virginia Tech, U.S.A.
Sinyong Choi, Ph.D., Kennesaw State University, U.S.A.

Keywords: cybercrime; artificial intelligence; deepfake; social engineering; metaverse

Abstract:
Artificial intelligence is one of the newest innovations which offenders exploit to satisfy their criminal desires. Although understanding cybercrime that is associated with this relatively new technology is essential in developing proper preventive measures, little has been done to examine this area. Therefore, this paper provides an overview of the two articles featured in the special issue of the International Journal of Cybersecurity Intelligence and Cybercrime, one about deepfakes in the metaverse and the other about social engineering attacks. The articles were written by the winners of the student paper competition at the 2023 International White Hat Conference.

Introduction

The advancement of technology is changing the way people interact in the world, and crime is no exception. Criminals develop and iterate on new illegal ventures. One of the recent technological innovations is artificial intelligence (AI). AI can perform tasks that typically require human intelligence by analyzing data, making predictions based on recognized patterns, and generating responses based on the vast amounts of information given to them (Choi et al., 2022). Offenders also exploit this human intelligence system to commit criminal activities, such as creating fake images and videos of someone to commit interpersonal cybercrime or enhancing the effectiveness of cyberattacks. This special issue addresses current criminal issues revolving around AI; one examines the victimization of deepfakes in metaverse and the other scrutinizes human vulnerabilities in social engineering attacks. The two papers are the winners of the student paper competition hosted by the 2023 International White Hat Conference. The following is a brief overview of each study.

Study 1

The paper titled Victimization by Deepfake in the Metaverse: Building A Practical Management Framework (Stavola & Choi, 2023) is an exciting addition to cyber victimization studies, researching personal cybervictimization in the metaverse. It bridges the gap between research on deepfake-related interpersonal crime and effective prevention methods. Conducting eight semi-structured interviews with policy, academic, and industry experts in South Korea, the authors used thematic analysis to identify themes in the expert testimonies on the topics of deepfake crime in the metaverse.

*Corresponding author
Katalin Parti*, Ph.D., Department of Sociology, Virginia Tech, 225 Stanger St, Blacksburg, Virginia, 24061, U.S.A.
Email: kparti@vt.edu

Routine activities theory and Eysenck's theory of criminality were used as theoretical frameworks to explain specific offender characteristics and target vulnerabilities to deepfakes. Participants suggested that motivated offenders in their 20s would likely commit crimes in the metaverse. The motivation for interpersonal cybercrimes includes financial gain or sexual gratification. It is suggested that money extortion and other financial crimes would become prevalent in the upcoming years. As per the suitable target aspect of routine activities theory, the research revealed that deepfake-related crime in the metaverse targets a younger population. For the capable guardians' aspect of the theory, experts suggested that proper guardianship is an effective way to mitigate cybercrime in the metaverse. The study reveals that deepfake interpersonal crime is a rising threat to the users of the metaverse. Therefore, it calls for establishing criminal procedures, police enforcement, and psychological healing programs for victims.

Study 2

The paper *Harnessing Large Language Models to Simulate Realistic Human Responses to Social Engineering Attacks: A Case Study* (Asfour & Murillo, 2023) contributes to the growing body of literature on how GPT can be utilized to simulate target responses to social engineering attacks. The authors utilize GPT-4 large language modeling (LLM) to simulate target vulnerabilities to social engineering (e.g., phishing) attacks. Using the Big Five Personality Traits model to categorize human personality traits, the authors find that personae with the qualities of naivety, carelessness, and impulsivity were particularly susceptible to attacks. That is, high agreeableness, low conscientiousness, and high neuroticism were associated with a higher susceptibility to social engineering attacks. In contrast, high openness to experience, extraversion, and other traits linked to agreeableness, and conscientiousness showed resistance against such attacks. The results of this study can inform the design of more sophisticated and precise cybersecurity systems, which could offer additional safeguards or warnings to individuals with high-risk personality traits.

Concluding Remarks

As criminologists, we are responsible for addressing criminal motivation and offering a comprehensive understanding of offending. This is especially important when the issues are closely associated with rapidly changing technology. These current issues are a good example of such efforts, focusing on a new technology that enhances our understanding of emerging cybercrime trends. We believe that the research findings and suggested preventive measures put forward in these articles will enhance the effectiveness of criminal justice policies and offer valuable insights for future criminological studies.

Reference

Asfour, M., & Murillo, J. C. (2023). Harnessing large language models to simulate realistic human responses to social engineering attacks: A case study. *International Journal of Cybersecurity Intelligence and Cybercrime, 6*(2), 21-74.

Choi, K., Back, S., & Toro-Alvarez, M.M. (2022). Digital forensics & cyber investigation. *Cognella.*

Stavola, J., & Choi, K. (2023). Victimization by deepfake in Metaverse: Building a practical management framework. *International Journal of Cybersecurity Intelligence and Cybercrime, 6*(2), 3-20.