International Journal of Cybersecurity Intelligence & Cybercrime

Volume 7 | Issue 2 Article 1

9-16-2024

Understanding the Use of Artificial Intelligence in Cybercrime

cybercrime, artificial intelligence, deepfake, social engineering, metaverse

Recommended Citation

Choi, S. , Dearden, T. & Parti, K. (2024). Understanding the Use of Artificial Intelligence in Cybercrime . *International Journal of Cybersecurity Intelligence & Cybercrime, 7(2)*, - . DOI: https://doi.org/10.52306/2578-3289.1185

Available at: https://vc.bridgew.edu/ijcic/vol7/iss2/1

Choi et al. (2024). *International Journal of Cybersecurity Intelligence and Cybercrime, 7*(2), 1-3.

Understanding the Use of Artificial Intelligence in Cybercrime

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

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

Abstract:
Artificial intelligence is one of the newest innovations that offenders also exploit to satisfy their criminal desires. Although understanding cybercrimes 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 articles featured in the special issue of the International Journal of Cybersecurity Intelligence and Cybercrime, ranging from deepfake in the metaverse to social engineering attacks. This issue includes articles that were presented by the winners of the student paper competition at the 2024 International White Hat Conference.

Introduction

With the fast advancement of technology changing the world in numerous ways, crime also evolves as offenders adapt to new opportunities and find innovative ways to carry out their illegal activities. One of the recent technological innovations is artificial intelligence (AI). AI can perform tasks that typically require human intelligence by analyzing vast amounts of 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 enhance the effectiveness of cyberattacks. Despite AI's immense potential to drive innovation and improve efficiencies, its application in criminal activities, such as creating deepfakes and conducting social engineering attacks, demands urgent attention from the academic and professional communities. Yet, the intersection of AI and cybercrime remains under-researched, leaving a gap in the understanding of how these technologies are exploited for malicious purposes. This special issue addressed current criminal issues revolving around AI; one examined the victimization of deepfakes in the metaverse, and the other scrutinized human vulnerabilities in social engineering attacks. The two published papers are the winners of the student paper competition hosted at the 2024 International White Hat Conference. The last article featured in this issue introduces a new theoretical framework to analyze factors influencing cybercrime. By exploring these topics, this special issue aims to shed light on the evolving landscape of cybercrime and propose innovative strategies for prevention and mitigation. The following is a brief overview of each study.

Study 1

The first study presents a comprehensive analysis of cybersecurity challenges in the healthcare sector (Praveen et al., 2024). This paper uses routine activity theory (RAT) to analyze high-tech cyber victimization case studies in the healthcare industry. The analysis explores the motivations of cyber attackers and t-

*Corresponding author
Katalin Parti*, Ph.D., Department of Sociology, Virginia Tech. 512 McBryde Hall, 225 Stanger St. Blacksburg, VA 24061, U.S.A.
Email: kparti@vt.edu

he characteristics of target companies, including value, inertia, visibility, and accessibility (VIVA framework), as well as inadequacies in cybersecurity guardianship. Based on the findings, the paper proposes preventive measures at three levels: technical solutions, legal and policy solutions, and measures to enhance awareness among employees about cybersecurity risks and best practices. Additionally, the study tests a comprehensive Digital Capable Guardianship Framework, an Online Lifestyle Awareness Framework, and a Policy Framework tailored to healthcare cybersecurity. The paper concludes by highlighting the need for a proactive, multi-layered approach to cybersecurity in the healthcare industry, emphasizing the integration of the VIVA components into these frameworks to enhance resilience against cyber threats.

Study 2

The second paper investigates the intersection of artificial intelligence (AI) and cybercrime, focusing on the risks, trends, and potential countermeasures (Shetty et al., 2024). Using routine activities theory (RAT) and its extension, cyber-routine activities theory (Cyber-RAT), the authors consider large language models (LLM) and AI-driven malware. The mixed-method approach provides both qualitative and quantitative analysis, summarizing findings related to AI prompts and expert interviews. The authors consider the need for increased awareness of how LLMs can increase cybersecurity risks. With increased capability, the need for better cyber hygiene is more important than ever.

Study 3

The last paper introduces the Integrated Model of Cybercrime Dynamics (IMCD) designed to analyze the complex interactions between individual traits, online behaviors, environmental influences, and the resulting cybercrime activities, both in terms of offending and victimization (Smith, 2024). The study details the model's conceptual foundations for ongoing research in cybercrime and highlights the model's flexibility that supports diverse applications, including policy, education, and intervention strategies.

Concluding Remarks

As criminologists, we have a responsibility to address criminal justice issues and offer a comprehensive understanding of them to the various actors in the criminal justice system. This is especially important when the issues are closely associated with rapidly changing technology, which brings about new types of crime that will necessitate quick responses and new counterplans by the criminal justice system. In this regard, the current issue is a good example of such efforts, which focused on one of the newest technologies to enhance our understanding of emerging cybercrime trends. This special issue contributes to the growing body of knowledge necessary for developing informed strategies and policies that address the dynamic nature of cyber threats. The studies presented herein underscore the importance of adopting a proactive and multi-disciplinary approach to cybersecurity, integrating technological solutions, policy frameworks, and educational initiatives to enhance resilience against AI-enabled criminal activities. By examining both the theoretical and practical aspects of cybercrime in the context of AI, these articles not only enhance our understanding of current threats but also pave the way for future research and policy development. It is imperative that researchers, practitioners, and policymakers collaborate to anticipate and counteract the ever-evolving tactics of cybercriminals. The insights gained from this issue are expected to serve as a foundation for ongoing dialogue and innovation in the field of cybersecurity, ensuring that society remains equp-

ped to protect itself against the emerging threats of the digital era. We believe that the research findings and suggested preventive measures put forward in these articles will not only enhance the effectiveness of criminal justice policies but also offer valuable insights for future cybercrime studies.

Reference

Choi, K., Back, S., & Toro-Alvarez, M.M. (2022). *Digital Forensics & Cyber Investigation*. Cognella.

Praveen, Y., Kim, M., & Choi, K. (2024). Cyber Victimization in the Healthcare Industry: Analyzing Offender Motivations and Target Characteristics through Routine Activities Theory (RAT) and Cyber-Routine Activities Theory (Cyber-RAT). *International Journal of Cybersecurity Intelligence and Cybercrime, 7*(2), 4-27

Shetty, S., Choi, K., & Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. *International Journal of Cybersecurity Intelligence and Cybercrime, 7*(2), 28-53.

Smith, T. (2024). Integrated Model of Cybercrime Dynamics: A Comprehensive Framework for Understanding Offending and Victimization in the Digital Realm. *International Journal of Cybersecurity Intelligence and Cybercrime, 7*(2), 54-70.