Article #2 Review: Understanding the Use of Artificial Intelligence in Cybercrime

Tay Lamell

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Prof. Diwakar Yalpi

November 17, 2024

Introduction and Goal

The article that I've chosen to review is *Understanding the Use of Artificial Intelligence in Cybercrime*. Despite being relatively short, the article takes aim at the use of artificial intelligence (AI) in cybercrimes, the article posits that not enough research exists on AI-based cybercrime prevention. Citing three studies that analyzed AI-based cybercrime in different ways, the article seeks to make a case for continued education and human centered cybersecurity are the best tools we have for stopping and preventing cybercrime.

Relation to the Material and a Look at Other Studies

Three studies are looked at by the article in an effort to support its claims, each of which analyze the world of cybercrime in different ways. The first of these studies analyzed the challenges that are faced by the healthcare industry as a result of cybercrime (Praveen et al., 2024). Here, the authors look at the motivations of cybercriminals, common characteristics amongst their targets, and existing weaknesses in said targets in order to discern how cybercrime impacts the healthcare industry. In the end, the authors came away with the idea that the best preventative measures included enhancing employee awareness in regards to cybersecurity risks and practices (Praveen et al., 2024).

The second study looked at in the article focused on AI-based cybercrime via risks, trends, and potential countermeasures (Shetty et al., 2024). Using an approach that allowed the authors to focus on LLMs and AI-based malware, the authors were able to gather qualitative and quantitative data to support their conclusion that there was a need for increased awareness of LLMs , as well as for "better cyber hygiene" (Choi et al., 2024). Taking a look at online behavior and cybercrimes that could occur as a result (Smith, 2024), the study analyzes the cyber attacker and the resulting victimization. Despite not much being discussed regarding the study itself, there is mention made of the Integrated Model of Cybercrime Dynamics (IMCD); it was stated that the IMCD supports a mix of approaches, including policy and education, to cybersecurity.

Conclusion

Ultimately the article concludes with the statement that the responsibility to arm ourselves against and better understand the ways that new technologies impact crime lies with criminologists. Each study was so because their findings support the belief that being proactive and staying informed (human centered cybersecurity) are the best ways to combat AI-based cybercrime. The article posits that doing so should be the leading option for cybersecurity, going on to say that, "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 equipped to protect itself against the emerging threats of the digital era" (Choi et al., 2024).

Citations

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

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