Article Review #2: Artificial Intelligence in Cybercrime: Artificial Intelligence in Cybercrime

Brandon A. Johnson

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

November 17, 2024

Artificial Intelligence in Cybercrime

The three studies discussed in this article explore the role of artificial intelligence (AI) in cybercrime and its implications for cybersecurity. These studies are connected to social science principles, such as understanding human behavior, motivations, and social structures. They examine how technology intersects with social patterns to shape cybercrime activities and explore how AI can both enhance and challenge efforts to combat these crimes.

The first study, by Praveen et al. (2024), looks at cybersecurity issues in the healthcare sector using Routine Activity Theory (RAT). It investigates the characteristics

of cyber attackers and the vulnerabilities of healthcare organizations, such as their value, visibility, and accessibility—key elements in the VIVA framework. The study's research questions focus on identifying why healthcare organizations are targeted and what preventive measures can be taken. Using case studies, the authors propose technical, legal, and policy solutions, as well as employee awareness programs to reduce cybersecurity risks. This study shows how RAT can help us understand how and why cybercrimes happen and suggests ways to prevent them in vulnerable sectors like healthcare.

The second study, by Shetty et al. (2024), explores the risks AI introduces to cybersecurity, especially through AI-driven malware and large language models (LLMs). The authors use both Routine Activities Theory and its extension, Cyber-RAT, to assess how cybercriminals can exploit AI tools. Their research raises concerns about the increasing sophistication of cyberattacks and the need for heightened awareness of AI's role in these threats. Through interviews and data analysis, the study emphasizes the importance of improving "cyber hygiene" and creating better defenses against AIenabled attacks. This study brings attention to how AI is reshaping the landscape of cybercrime and highlights the urgency of adapting cybersecurity strategies to these new risks. Smith's study introduces the Integrated Model of Cybercrime Dynamics (IMCD), a framework that looks at the complex factors driving cybercrime, from individual traits to online behaviors and environmental influences. The study focuses on both cyber offenders and victims, aiming to provide a holistic understanding of cybercrime and how it can be tackled through research, policy, and interventions. This model shows how

cybercrime is influenced by a mix of personal, social, and technological factors, offering a flexible tool for understanding the various dynamics at play.

Together, these studies provide important contributions to the field of cybersecurity by showing how AI and other technologies are transforming the ways cybercrime is committed and prevented. They highlight the need for a multi-layered approach to cybersecurity, with solutions ranging from technical fixes to better policies and increased public awareness. These studies also touch on the challenges marginalized groups face, especially regarding data privacy and security, emphasizing that these communities are often more vulnerable to cybercrime. Overall, the studies make a strong case for integrating AI in a way that not only addresses the risks but also strengthens societal resilience against emerging cyber threats.

References

Choi, Sinyong, et al. “Understanding the Use of Artificial Intelligence in Cybercrime.” *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 7, no. 2, 16 Sept. 2024, pp. 1–4.