Article Review #2

Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures

Kevin A. Loarca

Old Dominion University

CYSE 201S: Cybersecurity as a Social Science

Professor Woodbury

March 12, 2026

Article Review #2

The author provides an introductory of Artificial Intelligence (AI) and how technology has revolutionized every aspect of human existence. This also includes the misuse of AI in which it has become notorious in cybercrime. The study observes the relationship between AI and cybercrime, particularly in how AI can be exploited for malicious purposes (Shetty et al., 2024, p. 3). The research methods used for the research consist of both quantitative and qualitative approaches in examining the role of AI in facilitating cybercrime on both the clear and dark web (Shetty et al., 2024, p. 6). The quantitative method used was a collection of malicious AI-generated prompts across several online platforms. Additional evidence was collected that was written in different languages in which the researchers used Google Translate to translate messages (Shetty et al., 2024, p. 7). The data in this method was used to collect the number of prompts that served as malicious advice for others to use across a variety of online platforms. The analysis of this data highlights how cybercrime is a global issue as it extends beyond English-speaking communities (Shetty et al., 2024, p. 7). As for the qualitative data, interviews were done via Zoom with six experts in cybercrime, cybersecurity, and criminal justice. The data and analysis for the interviews began with open-ended questions to encourage broad and conceptual responses. Further in the interview, more structed questions were asked to gather specific information relevant to the study (Shetty et al., 2024, p. 7).

The hypothesis in the article is not directly stated, but it is implied with the authors' use of the Cyber Routine Activities perspective as the theoretical foundation. The perspective is similar to a theory called Routine Activities Theory (RAT). The RAT theory posits that criminal acts occur when three elements converge in space and time of motivated offenders, suitable targets, and the absence of effective guardians (Shetty et al., 2024, p. 4). To relate this to Cyber

Routine Activities, it emphasizes individuals' everyday routines on the internet, both vocational and leisure activities, increases the risk of computer crime victimization (Shetty et al., 2024, p. 5). Out of the three elements, the authors highlight the importance of guardianship as it ensures the cybersecurity of individuals when using the technology. It is also crucial for guardianship to have contextual awareness to distinguish between normal daily routines and criminal activities. As for the research questions, Shetty et al. (2024) seek to address three research questions which are:

> How is information involving malicious use of AI distributed and used on both the dark web and the clear web, and what are the mechanisms for its transfer between these domains? What role does media dissemination play in the spread of AI-facilitated cybercrime? How can individual cyber hygiene practices be improved to reduce the risks associated with AI-based threats? (p. 6)

These three research questions would be addressed throughout the paper. For the first question, the authors would answer this in their quantitative methodology when exploring different platforms. For the other two questions, they would be answered during the qualitative methodology as the interviewees answer their questions.

The paper has several connections to the materials learned in class. To relate to social science principles, three topics are included which are ethical neutrality, empiricism, and parsimony. For ethical neutrality, the researchers adhered to ethical standards to the participants during the interview. Specifically, they asked the interviewees whether they consent to providing their responses and contributions anonymously. For empiricism, the researchers studied behavior, which is real to the senses of sight and hearing. To be specific, the authors' quantitative methodology would show its visual demonstration and communication through

platforms to teach users to use AI to create malicious prompts. Lastly, parsimony is seen throughout the paper as the researchers provided their levels of explanation as simple as possible. For example, they provide background information, such as Routine Activities Theory, which would gradually be explained to make the necessary connections. Additionally, four concepts from class can be seen which are behavioral theory, psychology and awareness about cybersecurity, perceptions and safety, and limitations. For behavioral theory, the behavior is learned to produce malicious prompts through AI from peers across internet platforms. Then, for psychology and awareness about cybersecurity, it cannot be assumed that the users know enough about cybersecurity. That is why the importance of guardianship is needed to prevent users from engaging in cybercrime. This would also create a connection with the concept of perception and safety. Participating in those activities may appear to be "safe" to users unfamiliar with the prompt as they assume the AI prompt would not harm their own devices. Lastly, there were limitations present on pages twenty-three through twenty-four. One example of these limitations was during the translation and their use of Google Translate. Since there were language barriers during the research, they had used Google Translate instead of hiring a professional translator. There could have been mistakes during translation as Shetty et al. (2024) states "the non-English discussions on forums could have led to misinterpretations or a loss of nuance in the data" (p. 23).

The article provides several implications which cause concerns of marginalized groups. One group that can be influenced, especially without guardianship, is the youth with access to unrestricted internet. Not moderating the youth's activities online can be assumed to lead to dangerous paths. In this specific example, adolescents could find those AI generated prompts and could interact with them out of curiosity. Depending on how they react, it could open to

cybercrime opportunities. An additional concern of marginalized groups that can be affected is the elderly. With the low-entry barrier that AI now allows individuals to create automated attacks, scams can be produced quickly and effectively. With examples, such as voice cloning or deepfake videos, it has become more realistic which the elderly will be likely to be easily convinced. Overall, the article provides societal contributions that should be taken into consideration. The importance of moderation, both by developers and regulations, needs to be maintained. Developers need to update their AI programs to make sure to prevent circumvented prompts that allow malicious prompts from being produced. For regulations, laws need to be created and updated to address cybercrimes that are generated by artificial intelligence. A final contribution to the study is the unethical uses of the technology. As seen throughout the article, online platforms reveal how the technology can be misused and spread globally. This contribution would be an important factor to bring awareness that will lead to proper regulations.

References

Shetty, S., Choi, K., & Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. International Journal of Cybersecurity Intelligence & Cybercrime, 7(2). https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1187&context=ijcic