Name Chase McKnight

Date 02/20/2026

Article Review #1: Investigating the nexus between AI and cybercrime: dangers, trends, and mitigation strategies.

Introduction

S. Shetty, K.-S. Choi Park wrote the article "Investigatoring the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures," which was published in the International Journal of Cybersecurity Intelligence & Cybercrime in 2024. The research looks at how hackers are leveraging artificial intelligence (AI), a technology that is emerging swiftly, to make assaults stronger and how defenders might best respond. The research is particularly essential for current criminology, especially for understanding out how new technologies change how people commit crimes.

How it fits with the social sciences

This subject is closely related to social science concepts, since hacking is a socially ingrained phenomenon that encompasses human behavior, motives, societal structures, and institutional responses. The article makes use of Choi's (2008) Cyber Routine Activities Theory. This theory applies traditional criminological concepts to the contemporary digital landscape. This link explains how social science models may help us understand new kinds of crime that occurs online. We should look at how criminals choose their targets, how opportunities come up in everyday digital activity, and how social contexts change the behavior of cybercriminals.

Question for Research, Hypotheses, IV, and DV

The essay talks on a lot of key topics, such as:

How bad AI tools propagate on both the dark web and more well-known sites.

What the news can do to make crimes using AI more prevalent.

Good computing habits and safety measures may help protect you from AI-based threats.

The rationale behind this isn't the conventional manner of testing, but it is that increasingly complex and publicly accessible AI technologies make hacking more likely while simultaneously giving people better ways to protect themselves. If put into action as a variable:

The ability to get to and employ AI technologies in cyberspace is an independent variable (IV).

Dependent Variable (DV): How frequent and sophisticated hacking outcomes are made feasible by AI.

From this point of view, AI is transforming the abilities of criminals and the kinds of digital threats.

How the study was done

The authors used several research methodologies: utilized technologies like the TOR browser to go around the black web and find hazardous AI indications in 102 postings that may be utilized for attacks like malware and frauds.The qualitative section consists of interviews with six cybersecurity professionals to find out more about how attacks are developing and what the best ways to protect yourself are.

Different types of data and how to look at them

The numbers came from malware codes, suggestions, and examples of AI-generated attack pathways that were taken from sites. This evidence demonstrated that AI makes it simpler for hackers to get started and gives them more options for what they can target automatically. The in-depth talks made the data more meaningful by showing how it relates to real-world patterns, expert opinions, and the impacts of policies. Combining all of these kinds of data makes the study's outcomes better since it links real-world patterns with expert analysis.

How it relates to the ideas in the course

The article has to do with criminology principles like

Routine Activities Theory (RAT) says that thieves may easily discover appropriate targets in cyberspace when there isn't adequate oversight.

Environmental factors that lead to crime: illustrating how digital platforms and AI technologies influence the way things happen.

Social behavior and victimization: concentrating on how habits, knowledge, and proper online hygiene might increase susceptibility to assaults.

The research illustrates the need for the evolution of concepts within the social sciences in response to technological advancements.

Groups and Concerns on the Outside

The article reveals that AI-driven hacking impacts small firms, those with low incomes, and people who don't know much about how to defend themselves the most. A lot of the time, these organizations don't have the money or resources to create substantial walls, thus everyone is susceptible to assault. Access to technology, education, and safety in digital spaces is a more important problem of social justice.

Help for Society as a Whole

The research adds several important things, such as:

Discovering new hacking tendencies that are related to AI.

Bringing attention to the reality that AI may be both a threat and a protection.

leading groups and politicians to solutions that are founded on evidence.

Putting greater emphasis on how cyber hazards influence people's social life can help link what you learn about technology in cybersecurity with what you learn about crime.

This study shows how crucial it is to employ technology, policy, and social knowledge together to lower damage. This helps people prepare for future digital hazards.

To sum up

The research conducted by Shetty, Choi, and Park (2024) exemplifies the impact of AI on hacking and cybersecurity from an alternative academic discipline. This research enhances our comprehension of contemporary internet threats by integrating criminological theory with empirical data and expert opinions. It also offers strategies to prevent them and enhance individual resilience. It is a significant and pertinent contribution to cybercrime research, since it is grounded in social science, employs a mixed-methods approach, and focuses on populations who are often marginalized.

References

Shetty, S., Choi, K.-S., & 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/ijcic/vol7/iss2/3/