CHRISTIAN NIETO CYSE 201S 15 NOVEMBER 2024

ARTICLE REVIEW #2

The studies in this article look at how artificial intelligence is being used in cybercrime and how this is changing the way crimes like phishing and deep fakes are committed. These studies connect to criminology and sociology, which study crime and human behavior. They use a concept called Routine Activity Theory (RAT), which says crimes happen when there is a motivated criminal, a vulnerable target, and a lack of protection. The studies show how AI is making it easier for criminals to target people, especially those who are less aware of digital threats.

Each study asks different questions about how AI is affecting cybercrime. Study 1 (Praveen et al.) focuses on healthcare cybersecurity, asking what makes healthcare organizations easy targets for cybercriminals. Study 2 (Shetty et al.) looks at how new AI technologies, like large language models (LLMs), are being used by cybercriminals and how they increase the risk of cyberattacks. Study 3 (Smith) introduces a new model for understanding cybercrime, looking at how things like individual behavior and online actions lead to crime.

The research methods used in these studies vary. Study 1 uses case studies to understand how cyberattacks happen in the healthcare sector. Study 2 uses a mix of qualitative interviews and data analysis to explore how AI increases cybercrime. Study 3 introduces a new framework to study the relationship between personal traits and cybercrime. All three studies use data to show how technology and human behavior contribute to the rise of AI-driven crimes.

These concepts relate to criminology ideas, like Routine Activity Theory, which explains that crimes happen when certain conditions align. Study 3's Integrated Model of Cybercrime Dynamics builds on these ideas, adding new factors, like personal behavior and environmental influences, to explain cybercrime. These ideas are important for understanding how crime happens in the digital age.

AI-driven cybercrime also affects vulnerable groups, like older adults and people with limited access to technology. These groups are often targeted by AI-powered attacks like phishing or deepfakes, which can cause financial harm or emotional distress. The studies suggest that we need to create better awareness and policies to protect these groups from new threats.

In summary, these studies help us understand how AI is changing cybercrime and offer solutions to fight back. They stress the need for a multidisciplinary approach to deal with the rising threats. By raising awareness and proposing new solutions, these studies give us useful tools to stay ahead of criminals using AI to commit cybercrimes.