Gabrielle Gaston
CYSE 201

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

The article "Understanding the Use of Artificial Intelligence" addresses the rapidly advancing intersection between artificial intelligence (AI) and cybercrime. Cybercrime is a phenomenon that is growing attention and importance within the social sciences. As technology reshapes human interaction and societal structures, it also introduces an unimaginable amount of vulnerabilities and threats. This study directly engages with social science principles, particularly in understanding human behavior in digital spaces, criminal motivations, and systemic responses to emerging threats.

To begin, the research presented in this special issue includes three key studies. The first examines cybersecurity challenges in the healthcare sector using Routine Activity Theory (RAT) and the VIVA framework. This theory driven analysis focuses on factors like value, visibility, and guardianship to explain why certain healthcare organizations become targets of cybercrime. The second study explores how AI can be exploited in cybercrime through utilizing Cyber-RAT to analyze both qualitative and quantitative data targeting often large language models (LLMs). The final study introduces the Integrated Model of Cybercrime Dynamics (IMCD) by offering a new theoretical framework for analyzing how personal traits, digital behaviors, and environmental influences interact to shape cybercrime patterns.

Additionally, the methodologies across these studies are robust and varied, combining case studies, theoretical modeling, expert interviews, and data analysis. These approaches reflect the interdisciplinary nature of social science research, blending sociology, criminology, psychology, and information technology.

Gabrielle Gaston
CYSE 201

Professor, your PowerPoint presentations in class have discussed how technological change influences crime patterns. These ideas directly align with the article's frameworks and findings, illustrating the importance of applying theoretical knowledge to real-world scenarios. Module 3 references how normal users are usually not knowledgeable at making decisions about cybersecurity, being easily targeted by hackers. To mention, Module 6 references how experts have noted that "Internet deception is most perilous when the deceiver has constructed an environment that creates a trust and assurance in the relationship between the consumer and the deceiver". Module 10 picks up on the topic of deception through the elaboration on the influence of misinformation and disinformation. With the interaction between AI and users becoming more prevalent these PowerPoint references emphasize the importance of understanding AI and cybersecurity to further protect personal identifiable data and infrastructure.

Importantly, the article highlights how marginalized groups, such as patients in under-resourced healthcare systems, are especially vulnerable to cyberattacks. The misuse of deepfake technology and social engineering can disproportionately affect individuals who lack digital comprehension or access to protective tools. This further underscores the ethical and social justice dimensions of cybercrime prevention.

In conclusion, the studies in this article offer significant contributions to society by deepening our understanding of how AI can be both a tool for innovation and exploitation. They encourage proactive policymaking, ethical tech development, and public education to build safer digital environments for all.

Gabrielle Gaston
CYSE 201

References

Article: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1185&context=ijcic

Choi, S. , Dearden, T. & Parti, K. (2024). Understanding the Use of Artificial Intelligence in Cybercrime .

International Journal of Cybersecurity Intelligence & Cybercrime, 7(2),