The Future and Current Problems in the Cyber Environment

Aiden Johnson

CYSE201S

Article review 1

Diwakar Yalpi

9/28/25

The Relationship of study to Social Sciences

The reason this topic relates to the social sciences is that it focuses on scams, digital identity, and cyber victimization, which require an understanding of the human aspect to comprehend why they occur. The analysis in the article focuses on four studies that investigates cyber crime, governance, and digital threats to society (Kayser, C. S., Dearden, T., Parti, K., & Choi, S., 2025).

This article's research question addresses the "necessity of a multidisciplinary approach to address modern digital threats, bridging technical forensics, legal theory, and empirical research" (Kayser et al, 2025, p.1). The hypothesis proposes that more knowledge of the changing space of cybercrime is paramount to understanding these new and complex threats (Kayser et al, 2025).

The independent variable (IV) is to understand what actions we can take to lower the risk of harm in the cyber environment. The dependent variable (DV) is the safety and rights of online users. In other words, the harm that was caused because of actions we had done in the cyber environment (Kayser, 2025).

Article Analysis

In the first study Lim & Choi (2025) used a technical analysis to understand blockchain (a virtual database), where scammers use bitcoins and crypto coins to scam people out of money. Because of this, there is no tracking for the money.

The second study (Kayser et al. 2025) quoted (González-García Viñuela, 2025) to identify the legal side of analysis, "looking at the invasion of digital identity on a criminal law

side, with a focus on what is happening in Spain," (p.1) But it also focuses on the impact of a unified response around the world when it comes to cybercrimes (Kayser et al. 2025).

The third study is an analysis that focuses on Open Source Intelligence (OSINT). "Which found that users and other people were having potential problems, privacy problems, and bad use and collection of data on BellingCat, which is an OSINT website" (Pitman & Walsh, 2025). The data spanned from 2014 to 2024, during which time people experienced problems in the regions of the United States and Russia (Kayser et al. 2025). The people pushed for better legislation to protect OSINT websites and forums, aiming to keep users safe on these platforms (Kayser et al. 2025).

The final study uses the analysis of both qualitative and quantitative data, which looks into the Deviant Place Theory, "which says that people in a high-risk environment may have a high risk of victimization, even if personal behaviors are not a problem" (Grant & Gilreath, 2025). In this study, researchers recruited 924 internet users from Nigeria to assess whether they could modify categories of cyber offenses (Kayser et al. 2025). They reclassified cyber misuse as something encouraged by technology, and not by the need for technology to understand the connection between them (Kayser et al. 2025). The authors studied the connection between violent crime and property crime (Grant & Gilreath, 2025).

The study showed that the theory was accurate and that victimization rates are high in this context for cybercrime (Kayser et al. 2025). The study also found that "there should be more diligence for policymakers to reduce the cybervictimization here, and that more study and research needs to be conducted in the region on the problem" (Kayser et al. 2025, p.2).

Relationship to PowerPoint

Concepts from the CYSE201 (Module) PowerPoint include victimization and aspects of the Big Five personality traits. The first case involves blockchain and scammers. Scammers learn to use tricks to trick users into giving them their money through the use of the Big Five personality traits. The Big Five personality traits that scammers commonly exhibit here are agreeableness, extraversion, and openness to experience.

Openness to experience is an individual who is willing to take risks, such as engaging in activities that can put them at risk. They also tend to show agreeableness, sharing information with scammers, and making themselves more vulnerable. They are also extraversion, which is talking to new or more people than they should.

Goals of the article to help marginalized groups

The topic relates to the challenges, concerns, and contributions of marginalized groups. This article explores an understudied area in the world, with a focus on Nigeria and its challenges related to cybercrime victimization (Kayser et al. 2025). And the lack of studies and policymakers in this area of cybercrime victimization (Kayser et al. 2025). The study's overall contributions to society are that it addresses problems faced by marginalized groups in the cyber environment. It would be much better if we were more united on laws regarding cyber offenses, rather than having every place have its own rules that don't communicate with each other about the laws (Kayser et al. 2025). It also discussed open-source intelligence, a significant trend enabled by the internet. And what data, privacy, and risk are shared for a big or a bad thing (Kayser et al. 2025). And what skills scammers use to earn the trust of people so that they can get their money, and what money the scammers are most likely to want (Kayser, 2025).

Conclusion

In conclusion, this is an excellent article. It has some excellent points that will be significant in the future, as well as a few that are significant now. People need to understand the motives, theories, and principles regarding victims and professionals of cybersecurity because for now they will not go away.

References

González-García Vinuela, M. (2025). The Legal Response to the Intrusion into Digital Identity in Social Media. International Journal of Cybersecurity Intelligence & Cybercrime, 8(2). International Journal of Cybersecurity Intelligence & Cybercrime. https://doi.org/10.52306/2578-3289.1221

Grant, M., & Gilreath, T. (2025). Deviant place theory and adolescent victimization: Latent class profiles and mental health disparities in schools. APHA - APHA 2025 Annual Meeting and Expo; APHA. https://apha.confex.com/apha/2025/meetingapp.cgi/Paper/578822

Kayser, C. S., Dearden, T., Parti, K., & Choi, S. (2025). Navigating the Digital Frontier: New Perspectives on Cybercrime and Governance. International Journal of Cybersecurity Intelligence & Cybercrime, 8(2). International Journal of Cybersecurity Intelligence & Cybercrime. https://doi.org/10.52306/2578-3289.1222

Lim, A., & Choi, K. (2025). Modus Operandi and Blockchain Analysis of Romance Scams: Cryptocurrency-Driven Victimization. International Journal of Cybersecurity Intelligence and Cybercrime, 8(2). International Journal of Cybersecurity Intelligence & Cybercrime. https://doi.org/10.52306/2578-3289.1220

Nzeakor, O. F., Okafor, R. N., & Nwoke, C. N. (2025). A Study of Pattern of Cybercrime Abuse of Individual Internet Users in Umuahia North LGA, Abia State of South-eastern Nigeria. International Journal of Cybersecurity Intelligence & Cybercrime, 8(2). International Journal of Cybersecurity Intelligence & Cybercrime. https://doi.org/10.52306/2578-3289.1183

Pitman, L., & Walsh, L. (2025). Policy Considerations of Open-Source Intelligence: A Study of Bellingcat's Online Investigation Patterns (2014-2024). International Journal of Cybersecurity Intelligence & Cybercrime, 8(2). International Journal of Cybersecurity Intelligence & Cybercrime. https://doi.org/10.52306/2578-3289.1202 https://vc.bridgew.edu/ijcic/vol8/iss2/1/?utm_source=vc.bridgew.edu%2Fijcic%2Fvol8%2Fiss2%2F1&utm_medium=PDF&utm_campaign=PDFCoverPages