Solen Grossman

9/28/2025

Solen Grossman

School of Cybersecurity

CYSE201S - Cybersecurity and the Social Sciences

Article #1 Review: Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention

Solen Grossman

9/28/2025

BLUF

This review will discuss how the article “Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention” is just an overview of cybercrime and a discussion of best practices and cybercrime’s future, while downplaying its stated goal of exploring the psychological profile of criminals.

Introduction

I will be reviewing “Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention.” It was written by Duy Thuyen Trinh, Thi Cam Ha Dinh, and Thi Ngoc Kim Tran. The article frames itself as a psychological inquiry, however it ultimately fails to deliver on this premise due to creating a fundamental disconnect between its research question and its methodological execution, which is more of a general survey of cybercrime and resulting best practices rather than a focused psychological profile. This review will analyze this discrepancy by looking at the article’s brief discussions of social sciences and how they tried connecting it to cybercrime, or the lack thereof.

Article Overview

Ostensibly, this article is a systematic review intended to connect to social science through the topic of psychological profiling. It discusses these psychological elements in the section “Theoretical Perspectives on Cyber Security Crimes,” where it discusses criminological theories and how they guide cybersecurity professionals to more effective

and mitigation strategies. It discusses the theories of Routine Activity Theory, which suggests that crime occurs when there's a motivated offender, a suitable target, and an absence of capable guardianship and Deterrence Theory, which states that individuals are less likely to engage in criminal behavior if they perceive the costs outweighs the benefits (Trinh et al., 2025, p. 118-119). The article implicitly asks the question of what psychological traits define cybercriminals and how they inform the required prevention measures. The hypothesis is that psychological traits, which serve as the independent variable of this study, predicts engagement in cybercrime, which would be the dependent variable.

This article bases its study on 45 articles sourced from the following databases: PubMed, IEEE Xplore, Google Scholar, ACM Digital Library, and Web of Science. It captured a comprehensive range of studies on cybercrimes by using the following keywords and terms: "cyber security crimes," "cybercrime," "hacking," "phishing," "malware," "ransomware," "identity theft," "DDOS attacks," "cyber security strategies," and "cybercrime impact." It used various combinations with Boolean operators such as AND/OR to refine and expand the search results (Trinh et al., 2025, p. 116).

It included articles published between 2010 and 2023, using only articles from peer-reviewed journals that were relevant to cybercrime. It excluded articles from non-English publications, non-peer reviewed sources, and irrelevant to the focus of cyber security crimes. The article uses a systematic approach to extract relevant information by first initially screening the titles and abstracts, then doing a full text review. It used the tools EndNote to manage citations and references, Excel for creating a database of

extracted information, and NVivo to code and analyze the extracted data ((Trinh et al., 2025, p. 116-117).

The article assessed the quality of the included studies through the criteria of study design, sample size and representativeness, and bias and confounding factors. The article uses PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) to ensure the transparency and completeness of the reporting process and CASP (Critical Appraisal Skills Program) to critically appraise the quality and relevance of the included studies (Trinh et al., 2025, p. 117)

The article proceeds to discuss the evolution of cybersecurity threats and responses, including an overview of cybercrime milestones such as the Morris Worm, Melissa Virus, Love Bug, Operation Aurora, Stuxnet, and Wannacry Ransomware Attack. The article then goes to the aforementioned Theoretical Perspectives on Cyber Security Crimes section, which discusses Active Routine and Deterrence Theory alongside a third theory - International Cooperation Theory, which underscores global collaboration to combat cybercrime (Trinh et al., 2025, p. 119). It has a section discussing technological perspectives on cybercrime, including key principles of information security such as the CIA triad and safeguarding mechanisms for network security such as VPNs and SSL encryption.

The results and findings section discusses several case studies such as the Sony Pictures Hack of 2014, Target Data Breach of 2013, and Colonial Pipeline Ransomware Attack of 2021 (Trinh et al., 2025, p. 120-121). In the comparative analysis of the cases,

it noted there were shared elements but notable differences between the nature of the attacks and targeted sectors, such as how the Sony breach was state-sponsored espionage while the Colonial Pipeline attack involved ransomware. It gives solutions to mitigate these threats including multi-factor authentication and a culture of cybersecurity awareness through training programs to reduce human error and insider threats (Trinh et al., 2025, p. 122).

The article recommends that organizations should adopt a proactive and multi-layered approach to cybersecurity to mitigate risks and enhance resilience. It should enhance third party security by enforcing strict security compliance for third party partners, regularly audit their access, and implement continuous monitoring mechanisms to prevent unauthorized breaches. It argues that organizations should invest in advanced detection and response technologies. It also believes real-time threat intelligence, automated response systems, and AI-driven analytics are crucial for an organization's ability to preemptively detect, analyze, and neutralize cyberthreats (Trinh et al., 2025, p. 122).

The systematic review goes on after this, but beyond discussing the psychological impact of cybercrime on its victims, it simply ceases to even attempt to profile the attackers. It becomes a typical survey of the impacts of cybercrime, discussing its impacts such as financial losses to individuals, businesses, and governments, or the costs of prevention and mitigation, or privacy breaches and their implications, or business disruptions and loss of reputation, or legal regulatory consequences. It then discusses technological measures such as encryption and data protection, intrusion and prevention

systems, cybersecurity software and tools such as VPNs and multi-factor authentication, cybersecurity policies and best practices, employee training and awareness programs, incident response and disaster recovery planning, etc. It discusses challenges and future directions such as advanced persistent threats, AI and machine learning, and internet of things vulnerabilities. It discusses gaps in current research and future research directions, and then concludes.

Article Review

This article is fundamentally flawed because there is a critical disconnect between the proposed investigation and the actual executed analysis. The article has little to do with profiling of the psychology of cybercriminals and instead becomes a holistic discussion of the best policies to deal with cybersecurity, dealing little with the psychology of criminals. Cybercrime psychology is a social science matter, and beyond hinting it would discuss this, it doesn't do so. The abstract included the words "narcissism" and "impulsivity," which should have been examples of independent variables given the implied hypothesis, however these terms never appear again in the article. It describes the psychological impact of cybercrime on victims, but that's the furthest it goes.

In connecting the article to Cybersecurity and the Social Sciences, the article had an opportunity to discuss cognitive theories pertaining to traits such as narcissism and impulsivity (Which were mentioned in the abstract). While the article did briefly mention the motives of two of the case studies' cybercrimes, it didn't go further in constructing a psychological profile of them. An article that reflects the stated title and abstract should

have taken these case studies about the Sony breach, Target Hack, and Colonial Pipeline Ransomware attack and theorized about the likely psychological motivations and most applicable cybercrime theories to the believed modus operandi of the attackers. It didn't discuss how cultures that are marginalized may create the conditions for cybercrime justified through neutralization. For example, what were the goals of the North Korean attackers in the Sony breach? Was this monetary? Or revenge? How did they likely justify their actions, if at all? Did they believe the US deserved this? Did they believe their ideology was more important than the financial wellbeing of a foreign entity? No question like this is asked and there is no attempt at profiling the attacks.

As for the psychological impact of its victims, this article does discuss it further than the psychological profile of cybercriminals (Trinh et al., 2025, p. 125), but it still is insufficient. It discusses direct emotional reactions due to sustained cybercrime, but it doesn't discuss the psychological profile of those actually targeted by cybercrime. The article doesn't discuss how marginalized groups may be disproportionately targeted by cybercrime such as loan fraud or economic marginalization. It also doesn't discuss how a marginalized culture or climate may create the conditions for those marginalized people to conduct cybercrime themselves. In not discussing the damage of cybercrime to marginalized groups, it also doesn't discuss how they can be better protected from being victims of cybercrime or being induced into committing cybercrime themselves. The discussion of the psychological impact of cybercrime ends up being one paragraph of results of cybercrime amongst a list of several more. Given the article's title, this is a missed opportunity.

Solen Grossman

9/28/2025

Conclusion

In conclusion, while this article does contribute in surveying cybercrime and calling for more psychological insight into cybercrime and the best practices to fix these issues, the article betrays its initial premise of profiling the psychology of the actors in cybercrime. Rather than being a social-science dominated article discussing this psychological profile, it shifts to a general overview of cybercrime, its history, effects, and prevention methods. It pays minimal lip service to psychology and cybercriminal theories and suggests those should be considered, but beyond that is insufficient in its stated goals.

Annotated Bibliography

Trinh, D. T., Dinh, T. C. H., & Tran, T. N. K. (2025). Exploring the psychological profile of cybercriminals: A comprehensive review for improved cybercrime prevention. *International Journal of Cyber Criminology, 19*(1), 114–137 DOI: 10.5281/zenodo.47661906