Article Review #2: Exploring the Psychological Profile of Cybercriminals

Student Name: Alexander Walker

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/13/2025

Introduction/BLUF

In order to comprehend the psychological characteristics of cybercriminals and how these characteristics might guide improved preventative measures, this paper offers a comprehensive evaluation of 45 studies (Trinh et al., 2025). The BLUF argues that psychological traits like narcissism, impulsivity, and technical proficiency greatly influence cybercriminal activity, and that preventative measures must include psychological understanding in addition to technological protections (Trinh et al., 2025).

Connections to Social Science Principles

Many social science concepts, particularly those of psychology, sociology, criminology, and political science, are intimately related to this article. According to psychological perspectives, the writers emphasize how personality qualities like impulsivity and narcissism affect cybercrime (Trinh et al., 2025). In order to understand offender motivation and opportunity structures, they also make reference to criminological theories like routine activity theory and deterrence theory. The article is connected to sociology via social and cultural issues such as age, environment, and global digital inequality. International cooperation theory is mentioned in relation to public policy and political science.

Research Question, Hypothesis, and Variables

Research Question

What psychological characteristics are most prevalent among cybercriminals, and how may knowledge of these characteristics enhance the prevention of cybercrime? (Trinh et al., 2025)

Hypothesis

Preventive measures may be strengthened by identifying psychological qualities that cybercriminals share.

Independent Variable

Psychological characteristics (narcissism, impulsivity, technical skill, cultural background)

Dependent Variable

Cybercriminal behavior (offending type, technique, frequency, and complexity)

Research Methods

PRISMA principles served as the foundation for the authors' systematic review technique (Trinh et al., 2025). After screening 1,200 papers, they chose 45 peer-reviewed publications that were released between 2010 and 2023. PubMed, IEEE Xplore, the ACM Digital Library, Google Scholar, and Web of Science were among the databases.

Data Analysis Techniques

The authors used qualitative synthesis through **NVivo coding** to identify themes and patterns across studies (Trinh et al., 2025). They also employed CASP and PRISMA frameworks to assess study quality and eliminate low-rigor research. Findings were categorized into psychological traits, legal gaps, cybercrime types, and prevention strategies.

Course Concepts

Lessons on how human behavior influences cybersecurity vulnerabilities are reinforced in this essay. It reinforces the notion that cyberthreats are social failures impacted by opportunity, motivation, and psychology in addition to technological ones. The course's criminology modules are closely related to the application of ideas such as routine activity theory and deterrence theory (Trinh et al., 2025). The course material on cybersecurity policy and governance is related to the conversation about international cooperation and legal gaps.

Implications for Marginalized Groups

The article notes that psychological impacts of cybercrime—such as anxiety, fear, and emotional distress—often fall more heavily on vulnerable or marginalized populations who lack

resources for recovery, identity protection, or digital literacy (Trinh et al., 2025). It also discusses how victims of fraud or identity theft often face long-term emotional harm and economic consequences, especially those with fewer financial protections

Conclusion

In summary, this research provides compelling evidence that psychological profiling, in addition to technological safeguards, is necessary for preventing cybercrime (Trinh et al., 2025). It demonstrates how policymakers may create more successful regulations, training initiatives, and threat-reduction tactics by having a better grasp of the characteristics of offenders. In order to address the dynamic nature of cyber threats, the report also highlights the need of international cooperation and integrated preventive frameworks. In general, this study contributes to the social science understanding of why cybercriminals commit crimes and how society might more effectively avoid digital damage.

Reference

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.