# Psychological Profiles of Cybercriminals and Implications for Cybersecurity

Octavia Wade

Old Dominion University

CYSE 201S Cybersecurity and the Social Science

Professor Diwakar Yalpi

November 14, 2025

## Introduction

In the article, *Exploring the Psychological Profile of Cybercriminals: A Comprhensive Review for Improved Cybercrime Prevention* by Trinh, Dinh, and Tran (20225) gives an insight on systematic examination of psychological, social, and legal influences on the cybercriminal's behavior. By using what I learned so far in my CYSE201S class and the article, I can evaluate how this study is related to the social science principles, the research design, and the broader societal contributions while also connecting the key concepts like psychology, culture, subculture, and cyber laws.

## Social Science Framework and Relevance

In the article, it connects strongly with the social science principles due to its approaches to cybercrime as the number one product of human behavior, our social environments, and the cultural norms rather than the technical progresses. Trinh et al. (2025) told that "cybercriminal behaviors cannot be adequately understood with recognizing the complex interplay of psychological traits, social environments, and cultural influences." This concept can connect with Module 9 because it explains how culture can shape behaviors, feelings, norms, and expectations relating to cybersecurity and privacy. This article can also align with Module 12 because it highlights on the definitions of cybercrime can depend on the societal norms and legal frameworks rather than the purely technical factors; this can be seen in this point can be seen in the article from this statement "international cyber laws vary significantly, creating gaps that offenders exploit (Trinh et al., 2025)."

### *Research Questions, Hypotheses, Variables*

In the article, it gives out a guiding research question instead of using a testable hypothesis. This question is centered on naming the psychological traits displayed among cybercriminal offenders. It helps understand the traits that are related to behavior and study the

effects from legal environments on cyber offending. Trinh et al. (2025) talks about how psychological traits are influence from the cyber behavior, implying that “Impulsivity, narcissism, and cognitive distortions appear repeatedly across offender profiles in the literature.”

The independent variables are mentioned in the article study which include the traits from offenders, demographics, subcultural contexts, and environmental factors. On the other hand, the dependent variable involves cyber offending behaviors, their interior motivations, and ways to prevent these outcomes. This insight can relate to Module 5’s discussion on personality traits and cognitive processes that can shape the cyber offender; for example, impulsivity, techniques from the neutralization standpoint, and learned behavior patterns.

***Research Methods***

Trinh et al. (2025) uses the PRISMA-Based to systematic review methods; they described this process as “a structured, transparent, and replicable review of peer-reviewed studies published between 2010 and 2023.” In the researchers' article, they found over 1,200 studies; however, they narrowed it down to only 45 through inclusion and exclusion criteria. Trinh et al. (2025) used EndNote to reference the management, Excel for coding and extracting data, and NVivo for thematic analysis. You can consistently see this in the social sciences because it shows structured evidence of synthesis and rigorous methodological transparency.

**Types of Data and Analysis**

In their data, both qualitative and quantitative data are used. This includes empirical studies from offender traits, incidents from case studies in cybercrime, and an analysis on the global legal frameworks. Trinh et al. Applies the thematic coding, by talking about “recurring themes such as impulsivity, technical proficiency, and moral disengagement emerged during NVivo analysis.” This method can correspond with Module 12 because it talks about how to

analyze cybercrime through a clear operational definition and systematic frameworks to avoid any overlap or ambiguity in identifying offenses.

***Connections to Course Concepts***

This article directly complements the theories and concepts; this can be presented in Module 5. It emphasizes on how offenders rely on their cognitive distortions, and the article states that, "cybercriminals frequently rationalize their actions by minimizing harm or depersonalizing victims (Trinh et al., 2025)." This concept can algin with Neutralization Theory. In Module 5, we discuss how impulsivity is a key risk factor, which can connect with article reinforces about how nothing can appear as impulsivity as "one of the most consistently reported traits across studies of cyber offenders (Trinh et al., 2025)."

In CYSE201S, we discussed the coverage of cyber subcultures that can also be reflected strongly in the article. Trinh et al. (2025) stated that "online communities often serve as breeding grounds for emerging cybercriminals, offering both technical guidance and social validation." This concept mirrors the course's depiction of hacker culture, networks from criminals, and how groups of norms can impact an individual's behavior.

Themes from Module 12 can reflect cyber law and the discussion of legal inconsistencies. Trinh et al. (2025) states "lack of harmonized cybercrime legislation creates safe havens for offenders and complicates international investigations." This can connect with Module 12's discussion about how different national frameworks delay global cybersecurity enforcement.

***Challenges and Concerns for Marginalized Groups***

In thought the researchers did not explicitly talk about their finding centered around marginalized populations, it did mention the implications from disproportionate impact on vulnerable groups. Trinh et al. Highlights on the victims with a lower digital literacy are most

likely to be hackers' frequent targets; they noted that “individuals with limited cybersecurity awareness face heightened risk of exploitation.” This can be explained in Module 5 because it talks about how groups that experience lower digital literacy or resource can suffer psychological consequences after being impacted by victimization; this includes emotions like fear, anxiety, and helplessness.

The article notes how the economic and social disparities can push individuals to do cybercrime, stating how “socioeconomic disadvantages and restricted legitimate opportunities can contribute to cybercriminal involvement especially among youth (Trinh et al., 2025).” In Module 9, it also gives an example of how cybercriminal subcultures can emerge from the economically marginalized regions.

***Contributions of the Study to Society***

Trinh et al. (2025) made a significant contribution that is related to research, policy, and practice. It blended in the psychological and cultural perspectives while also encouraging the study of policymakers and how they develop prevention strategies that can go beyond the traditional technical defense. Trinh et al. (2025) noted that “effective cybercrime prevention must incorporate psychological insight, legal reform, and international cooperation.” The researcher also provides a foundation on how to strengthen global legal frameworks; it also reinforced from the course principles on how cybersecurity is fundamentally a human problem, not necessarily a technological problem.

***Conclusion***

Overall, this article gave me comprehensive insight into understanding cybercriminal behavior by emphasizing psychological traits, influences from cultural, and legal challenges. Through their approach to systematic and keeping an interdisciplinary focus, it helped me

support key concepts that were covered in my CYSE201S course. It mainly regarded psychological motivation, subculture influences, and legal complexities. Trinh et al. (2025) highlighted on how contributing more effective, human focused on cybersecurity strategies and how it can further improve the importance of integrating different social perspectives with other cybersecurity research projects and practices.

# References

CYSE201S Module 5: *Applying Psychological Principles of Cyber Offending, Victimization, and Professionals.*

CYSE201S Module 9: *Culture, Social Media and Cybersecurity.*

CYSE201S Module 12: *Conceptualizing Cybersecurity as a Crime- Part 1.*

Trinh, D., Dinh, T. C. H., & Tram, T. N. K. (2025). *Exploring the psychological profile of cybercriminals: A comprehensive review for improved cybercrime prevention.* Internation Journal of Cyber Criminology, 19(1), 114-137. View of Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention