

**Article Review #2: Review of Exploring the Psychological Profile of Cybercriminals: A  
Comprehensive Review for Improved Cybercrime Prevention**

Student Name: Melissa Gaskins

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Dr. Jordan Quinn

Date: 04/07/2026

### **Introduction/BLUF**

This article discusses a study which examines the traits of cybercriminals to assist in preventing future acts of crime. The study finds that certain traits and attributes such as narcissism, impulsivity, and high technical proficiency contribute to cybercrime (Trinh et al., p.114).

### **Relation/Connection to Social Science Principles**

This article relates to many of the seven principles of social sciences. It relates to empiricism by basing the study on existing evidence rather than using opinions or hunches. Determinism, which is the principle that means that behavior is determined by preceding events, is used in the study by showing that cybercriminals may participate in cybercrimes due to behavioral and psychological traits. Relativism, which is the principle that means that all things are related, is used by determining that psychological traits can relate to criminal behavior in cyberspace.

### **Research Question /Hypothesis/ Independent Variable/Dependent Variable**

The main research questions the article and study address are: What psychological traits and behaviors do cybercriminals tend to have? How can that information be used to assist in preventing cybercrime? The hypothesis proposed by the authors seems to be: People with various psychological and behavior traits are more likely to take part in cybercrime. Since personality traits can lead to increased risk of participating in cybercrime, the traits are the independent variable. The dependent variable, which is caused by the independent variable, is the criminal behavior.

### **Types of Research Methods used**

The study used multiple search strategies including archival research and case studies. In the article, the authors use archival research, which is the use of archives to conduct scientific studies, by reviewing information from several databases and digital libraries (Trinh et al., p.116). They also used case studies of the Sony Pictures Hack of 2014, the Target Data Breach of 2013, and the Colonial Pipeline Ransomware Attack of 2021 (Trinh et al., p.120-121). Since the article uses both case studies and archival research, the study mainly uses qualitative research methods.

### **Types of Data Analysis used**

According to the article, the data analysis techniques used by the authors include study design, sample size and representativeness, and bias and confounding factors (Trinh et al., p.117). Study design is described as “the methodological rigor of the studies”. Sample size and representativeness is described as the “adequacy of the sample size and the representativeness of the study population”. Lastly, they describe Bias and Confounding Factors as “the assessment of... biases... that could affect the study” (Trinh et al., p.117)

### **Connections to other Course Concepts**

Module five concepts are greatly reinforced by this study. Both the article and module five focus on how certain factors or traits influence cybercriminal behavior. The lecture discusses different theories as to why criminals may engage in cybercrime such as cognitive, behavioral, and personality theories (Module Five, Slides 5-8). The article also discusses various theories such as routine activity theory and deterrence theory (Trinh et al., p.118). These theories go well with the articles focus on how traits can affect criminal behavior.

### **Connections to the Concerns or contributions of Marginalized Groups**

According to the article, the study finds that criminals often show behaviors of various psychological traits “with variations based on crime type, age, and cultural background (Trinh et al., p.114).

### **Overall societal contributions of the study/Conclusion**

In conclusion, the article contributes to society by studying behaviors to prevent cybercrime victimization. It advances our understanding of cybersecurity and social sciences by conducting a study to improve overall understanding of cybercrime and cybercriminal behavior to prevent further crime in cyberspace.

## Reference

TRINH, D. T. (2025, June). *International Journal of Cyber Criminology Vol 19 issue 1*

*January – June 2025. Cyber Crime Journal.*

<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/download/452/133/909>

[View of Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention](#)