Article Review #1: Exploring the Psychological Profile of Cybercriminals:

A Comprehensive Review for Improved Cybercrime Prevention

Student Name: Kennice Allea Balmoria

School of Cybersecurity, Old Dominion University

Instructor Name: Professor Diwakar Yalpi

Date: 20 February 2026

Introduction/BLUFF

This article, Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention (Trinh et al., 2025), examines the psychological traits that influence cybercriminal behavior and how these traits can inform better prevention strategies. **Bottom line up front:** The authors conclude that cybercriminals commonly exhibit traits such as narcissism, impulsiveness, and high technical proficiency, and that integrating psychological insights into cybersecurity policy is essential for effective prevention.

Relation to Social Science Principles

The article strongly reflects the seven principles of social science:

- **Relativism:** Cybercrime is shaped by interconnected systems: technology, economics, politics, and society. The authors note that cyberattacks have "cascading effects across multiple sectors," showing how systems influence one another.
- **Objectivity:** The study uses a systematic PRISMA review, ensuring unbiased, scientific analysis.
- **Parsimony:** Despite reviewing 1,200 studies, the authors identify a small set of recurring traits (narcissism, impulsivity, technical skill) that explain much cybercriminal behavior.
- **Empiricism:** Findings are based on 45 peer-reviewed studies, case analyses, and coded qualitative data.
- **Ethical Neutrality:** The authors analyze offenders without judgment, focusing on understanding behavior rather than moral evaluation.
- **Determinism:** Psychological traits and environmental factors can influence cyber offending, showing that behavior is not random.

- **Skepticism:** The review evaluated the quality, bias, and limitations of existing studies.

Research Question/Hypothesis/Independent & Dependent Variables

Research Question:

What psychological traits characterize cybercriminals, and how can understanding these traits improve cybercrime prevention?

Hypotheses:

1. Cybercriminals share identifiable psychological traits.
2. These traits vary by crime type, age, and cultural background.
3. Understanding psychological traits can improve prevention strategies.

Independent Variables

Psychological traits, age, cultural background, and type of cybercrime.

Dependent Variables

Cybercriminal behavior, likelihood of offending, and type of offense committed.

Types of Research Methods Used

The study uses a systematic literature review, which is a social science research method. This is primarily qualitative, with structured coding and thematic analysis, and it includes:

- PRISMA screening
- Inclusion/exclusion criteria
- Full-text analysis
- Archival research (existing studies, case reports, legal documents)

Types of Data Analysis Used

The authors used:

- NVivo qualitative coding to identify themes
- Comparative case analysis (Sony, Target, Colonial Pipeline)
- Content analysis of psychological traits
- Quality assessment tools (CASP & PRISMA)

The analysis synthesizes psychological, criminological, and technological findings.

Connections to Course Concepts

- **Module 2 (Principles of Science):** Uses empiricism, objectivity, determinism, and parsimony.
- **Module 3 (Research Methods):** Systematic review = archival research; case studies reinforce course examples.
- **Module 4 (Human Factors & Psychology):** Discusses impulsivity, narcissism, cognitive distortions, and victim psychology.
- **Module 5 (Cyber Offending):** Aligns with Dark Triad traits, motivations (money, revenge, curiosity), offender cognitions.

Connections to Concerns or Contributions of Marginalized Groups

- Unequal victimization risks for populations with limited cybersecurity resources.
- Global disparities in cybercrime laws leave some countries more vulnerable.
- Cultural differences in offender traits and motivations.
- Psychological harm that disproportionately affects vulnerable groups.

- **Victims of Cybercrime:** Victims experience stress, anxiety, fear, and emotional distress, which disproportionately affects people with fewer resources or support systems. Like low-income individuals, elderly people, people with limited digital literacy, and women targeted in cyberstalking or harassment.
- **Small and Medium-Sized Enterprises:** SMEs are considered a marginalized economic group because they have fewer cybersecurity resources, face disproportionate financial damage, and are often excluded from large-scale cybersecurity infrastructure.
- **Privacy-Vulnerable Populations:** In the article, they discussed major privacy breaches that disproportionately harm people with low digital literacy, social media users unaware of data exploitation, and individuals in politically targeted groups.
- **Employees in Organizations Targeted by Cyberattacks:** Employees become marginalized when their personal data is leaked. These employees often have no control over corporate cybersecurity, face reputational harm, and experience job insecurity after breaches.
- **Populations Affected by Critical Infrastructure Attacks:** The Colonial Pipeline attack caused fuel shortages and panic buying, which harmed low-income communities, rural communities, and people with limited transportation options.
- **Individuals Targeted by Online Fraud and Scams:** The article discusses foreign-based fraud and deceptive online schemes. These affect elderly individuals, immigrants, people with limited English proficiency, and low-income individuals.
- **Countries with Weaker Cybersecurity Infrastructure:** The article mentions global inequalities in cybercrime prevention and cooperation. This implies marginalized

geopolitical groups like developing nations, countries lacking cyber-law enforcement, and nations excluded from international treaties.

Overall Societal Contributions/Conclusions

This study contributes significantly to society by identifying psychological traits linked to cyber offending, highlighting gaps in legal frameworks, and recommending the integration of psychological insights into cybersecurity policy. It advances understanding of cybercriminal behavior, emphasizes the need for international cooperation, and provides actionable guidance for policymakers and cybersecurity practitioners. By combining psychological, criminological, and technological perspectives, the article strengthens the foundation for more effective cybercrime prevention strategies.

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

Article Link: https://www.cybercrimejournal.com/