Name: Shaun Farmer

Sept. 28th, 2025

Article Review #1: Exploring the Psychological Profile of Cybercriminals

BLUF

Trinh, Nguyen, Pham, and Vu's (2025) recent article, Exploring the Psychological Profile of Cyber Criminals: A Comprehensive Review for Improved Cybercrime Prevention, is a systematic literature review study about common psychological traits of cyber offenders and the many-layered solutions necessary to prevent cybercrime. Bottom line: most cyber offenders have narcissistic, impulsive, and/or Machiavellian personalities in addition to technical skills. A better understanding of the offenders' psychological and social profiles, as well as both the potential target vulnerabilities and potential impacts of different types of cyber incidents and threats, can better inform more robust prevention, stronger responses, and more effective resilience and continuity strategies at both organizational and global levels (Trinh et al., 2025). There is also strong overlap with the social science of cybersecurity, as the study shows how aspects of human behavior and personality are leveraged or exploited in the majority of cases of cybercrime.

Relation to Social Science Principles

This article very clearly relates to the social sciences by providing a detailed analysis of cybercrime that frames it in terms of human behavior, individual and social psychological traits, and broader political, environmental, and societal factors. Cyberattacks are not just technical attacks on software, hardware, and networks; they are also, in most cases, criminal attacks enabled by both the potential target vulnerabilities and potential impacts of different types of

cyber incidents and threats and by human opportunities or behaviors (Trinh et al., 2025). Routine Activity Theory is used to describe the roles of opportunity and exposure, as motivated offenders are able to commit their crimes because there is often a lack of capable guardians and most targets are always “online” (Trinh et al., 2025). The Dark Triad of personality traits (narcissism, Machiavellianism, and psychopathy) is also used as a theoretical framework for understanding offender motivations and drives as social-psychological phenomena.

Research Question, Hypotheses, and Variables (IV & DV)

The primary research question used in Trinh et al. (2025) is “What psychological and social characteristics are most common among cybercriminals, and how can this knowledge improve prevention strategies?” It can be inferred that the author’s implicit theory/hypothesis is that offenders will have predictable traits (e.g., narcissism, impulsivity, Machiavellianism) that affect their behavior and that these variables can predict cybercrime patterns. The IVs are offender traits (narcissism, impulsivity, level of empathy), demographic factors (age, education, gender), and technical skill. The DV is cybercrime involvement, operationalized by type, frequency, or severity of offenses committed. For example, high impulsivity or low empathy (IVs) may be associated with higher likelihood of disruptive cyberattacks (DV). The article’s design frames the psychological and demographic factors as causal (i.e., actually influencing criminal behavior). This reflects how social science is used to explain the real-world impact of variables related to human thoughts, feelings, and interactions.

Research Methods Used

Trinh et al. (2025) used a systematic literature review method to answer the research question, which is very similar to the PRISMA method that we covered in class. Their inclusion criteria were more structured and formalized to capture only articles, datasets, theories, case studies, and other research resources that were relevant to the profile of cyber criminals. In addition to the theoretical review process, this method also included other research methods, such as surveys and interviews, when assessing prior research and results. They largely followed a similar process as we did in the pre-Classroom class assignment by searching for individual studies using a broad search strategy, but they also used the references of prior reviews and other resources in their field to source additional research. As in our classroom activity, this process of searching for existing literature allowed for the creation of a narrative analysis and identification of research gaps in the available literature.

Data and Analysis

The data in this study is that of previous research articles, interviews, surveys, personality and competency assessments, security incident case reports, and other resources that could provide insight on cybercriminals. The articles and case reports were then analyzed both quantitatively and qualitatively to identify common patterns, results, and characteristics of cybercriminals. Quantitative findings included offender self-reported data as well as prevalence or other statistical data. Qualitative data included case reports and other narrative accounts that described past incidents and responses. Trinh et al. (2025) found common offender characteristics including thrill-seeking behavior, low empathy, and high technical skill. They also

found that most prior research data on cybercriminals is limited, self-reported, or out of date due to the rapidly changing nature of the field.

Connections to Course Concepts

This article strongly connects to several concepts in our class. The mention of Routine Activity Theory is a direct connection to one of the classical criminological theories that we covered and which explain how cybercrime can happen. The Dark Triad is a psychology and behavioral theory we also discussed, and the article also relates to our discussions on the psychology of offenders. The mention of "human" and "human factors" vulnerabilities and aspects of incident prevention and response connects directly to our lessons on the social science of cybersecurity. The article's references to regulations and statutes like GDPR and CISA, as well as international organizations like INTERPOL, are also directly connected to many of our concepts and topics related to law, policy, and governance in cyberspace. Overall, this article strongly connects to many of our core concepts.

Marginalized Groups: Challenges and Considerations

The study did not directly focus on marginalized groups, but the findings of this research have several important implications for these communities. It is a key part of our vulnerability identification, prevention, and awareness training processes to identify marginalized groups that are less aware of these issues and more vulnerable to cybercrime. Examples include marginalized populations at higher risk of cyber victimization such as social engineering, phishing, identity theft, and financial fraud. Small and medium-sized enterprises (SMEs) can also be considered a

marginalized group in a broader business context, as SMEs have fewer resources and are at higher risk of cyberattacks. In the global context, there are also significant disparities in digital infrastructure and cybersecurity resources, so developing countries can be seen as a vulnerable or marginalized group. Although this article does not directly mention marginalized groups, it is still important to ensure that prevention measures and awareness programs are accessible to all segments of the population, and that under-resourced or otherwise marginalized countries are included in global cooperation and capacity building.

Overall Contributions of the Study to Society

The study is useful for society in several ways. First, it contributes to our body of knowledge about the profile of cybercriminals and offers theoretical and practical insight on which aspects of psychological traits could be used to both inform prevention and strengthen our responses and organizational continuity measures in case of incidents. Second, this study's prevention recommendations connect to larger efforts to design layered, multi-pronged, and multi-level approaches to defending against cybercrime that combines all stakeholders and resources. Third, this study also points to areas where more or better research is needed, including on the long-term impacts of different types of cyber incidents and how emerging or disruptive technologies such as AI, IoT, quantum computing, and next-generation wireless affect cybercrime. Fourth, by conceptualizing cybercrime as a social and psychological problem as well as a technical one, this study also contributes to wider societal understanding of cybersecurity issues.

Conclusion

In conclusion, this article is a useful and significant contribution that relates cybercrime to both psychology and criminology, as well as cybersecurity and social science. The article relates to social science principles both in its framing of cybercrime and its analysis of key concepts in social science as they are related to cybercrime. The authors have applied a systematic review methodology in order to include more studies and to provide a more comprehensive literature review of existing research. There are several direct connections between the findings and concepts we discussed in our class. There are also strong and direct implications for marginalized groups, as they are often more vulnerable to cybercrime and have less access to mitigation or awareness resources. In summary, this article has provided useful contributions to the social science of cybersecurity, as well as practical value to those responsible for cyber risk management and incident response in various organizational and national contexts.

Reference

Trinh, H., Nguyen, T., Pham, L., & Vu, M. (2025). Exploring the psychological profile of cyber criminals: A comprehensive review for improved cybercrime prevention. International Journal of Cyber Criminology, 19 (1), 128–137.
https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/452/133