Article Review #1: Psychological Profile of Cyber Criminals Review

Student Name: Liangshun Cheng

School of CyberSecurity, Old Dominion University

CYSE 201S: Cyber Security and the Social Sciences

Instructor: Diwakar Yalpi

Date: 2/19/26

Introduction

The Academic Article titled View of Exploring the Psychological Profile of Cyber Criminals: A Comprehensive Review for Improved Cybercrime Prevention is an academic paper that goes over the Psychological traits, motivations, and behaviors exhibited by Cybercriminals. While also arguing for the inclusion of these human behaviors in investigations and into the legal system for Cybersecurity.

Relation to the Principles of Social Science

This article relates very closely with the seven principles of social science mentioned in class, those being relativism, objectivity, Parsimony, Empiricism, Ethical Neutrality, Determinism, and Human Behvior. Though the article itself pulls on a few specific principles more so then others. For instance, in Empiricism, most of the data here is empirical, over a thousand studies and case studies like the Sony Pictures Hack of 2014, the Target Data Breach of 2013, and the Colonial Pipeline Ransomware Attack of 2021. Then there's Human Behavior as the article itself states its exploring the Psychological Profile of Cybercriminals, and the impacts of cybercrime on victims. Finally, Ethical Neutrality, as the article only explains what Cybercriminals do, how they think, and the effects on victims depending on what happened, not once did they bring morals or ethics into this, sticking strictly to gathered and provided data.

Research Question/Hypothesis

The research question proposed by this article is what kind of psychological traits are present in Cybercriminals and how could this be used to prevent criminal action. The Hypothesis of this document is that Cybercriminals share psychological traits that can help cybersecurity professionals prevent attacks. The Independent Variable in this document is the psychological

traits possessed by cyber criminals, and the Dependent Variable is the prevention strategies that cyber professionals come up with, as well as future criminal behavior once these strategies can be implemented.

Research Methods

Archival Research was the biggest method used throughout this article. Having used a quantitative data method. However, the authors and researchers set conditions on what could be used. Firstly, articles used must have been published between 2010 and 2023 to make sure it was relevant. Secondly, all articles had to be published in peer-reviewed journals to ensure they were credible. Finally, the article in question must be relevant to Cyber Security Crimes, specifically types of crime, the impact of said crime, and prevention strategies. The researchers also had criteria where they would ignore documents. For example, if the article was not originally in English, they would ignore it due to the possibility of translation messing up the original meanings. They also ignored non-peer-reviewed sources such as magazines, blogs, and opinion works. Finally, they ignored articles that were not specifically related to cybersecurity crime to keep all information on topic.

Types of Data/Analysis

According to the paper, a systematic approach was taken to extract data from the studies they used. They looked at titles and abstracts of the article to check if the article may be relevant before reviewing the full text and pulling out the necessary information. To ensure the reliability of the data collected, they looked at how the research in the papers they gathered and made sure they were robust in data collection and methods of analysis. They also made sure to gather a large enough sample size when it came to data in order to try and include the factor of

population, and as such, different sections of life. Finally, to spot and mitigate bias that could potentially exist in these articles and to ensure transparency and compleatness the researchers used PRISMA or “Preferred Reporting Items for Systematic Reviews and Meta-Analyses”.

Connection to Course

This article connects especially well with CYSE 201S, Cyber Security and the Social Sciences, as both is article and the class looks at Cyber Security more on the human side of things instead of the technical. We were also able to apply research methods and analisis of Cyber Security research we learned in this course to analyze this article. Techniques like different research methods we learned in earlier modules, and through that, we can spot the sections that we were taught. The article also dives into the Psychological side of cybersecurity and common traits between cybercriminals, and their effects on victims.

Possible Connection to Marginalized Groups

The article itself does not really mention marginalized groups; however, age and upbringing are stated to have an effect on psychological traits that could be present in cybercriminals.

Conclusion

In conclusion, this article highlighted and granted us a better understanding of cybercriminals and their psychology, and shared alongside strengthening prevention strategies used to combat cybercrime. It also supports having a better legal and international framework for going after cybercrime and raises awareness of cyber threats by providing examples of threats attacking systems like Sony. It argues for International corroboration, better understanding, and

use of cybercriminal psychology in investigations, and that parties must keep themselves secure online.

Works cited

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