

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

By: Kayle Glaize

School of Cybersecurity

CYSE 201S: Cybersecurity and Social Science

Professor Matthew Umphlet

August 2 2026

The article *Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention* explores the idea that understanding the psychological traits of cybercriminals is just as important as understanding the technology behind the attacks and how they are used to carry them out. The article argues that while researching and developing new technologies are essential to combating cybercrime as it happens, having a grasp of the human behavior behind these acts is vital if cybercrime is to be stopped before it even occurs. They argue that, because cybercrime is growing so quickly in both frequency and complexity, it should be treated as a global issue that spans economic, social, psychological, technological, and legal studies.

This article is related to the principles of social sciences because it focuses on the human behavior that is behind why these cybercriminals do what they do. This study asks questions like why people turn to cybercrime and what their motivations are, whether cybercriminals all share psychological traits or whether they vary from type to type, and whether understanding the psychology behind cybercrime actually helps prevent it from happening. Throughout the article, the authors stress that the current approach to researching cybercrime and cybersecurity fails to represent social sciences, specifically psychology, properly and that the goal should be to incorporate both the technical and psychological aspects to create a deeper and more robust understanding of the issue of cybercrime.

To answer their questions, the authors chose to conduct a systematic literature review, meaning they collected a multitude of previous studies relevant to their topic and analyzed the study itself quality and the subsequent results of each one. They chose to

follow PRISMA guidelines, which are a set of globally recognized rules that help in organizing and creating systematic reviews while also preventing researchers from relying only on certain options/finding they agree with because they are required to share things like where they collected their articles, why studies were disqualified from the research, etc. Because there are already many studies that have been conducted on the psychology behind cybercrime, the authors decided to search through many academic journals and databases, over 1,000 studies total from multiple databases such as Google Scholar, PubMed, IEEE Xplore, and more. They narrowed in on 45 articles and studies on the psychology behind cybercrime and used them to create conclusions on things such as common motivations and behavioral traits. The articles the authors reviewed included case studies, research on psychological traits, the current legal framework in place to provide and regulate cybercrime, and behavioral patterns, psychological traits, and motivations of known cybercriminals; as the authors were reviewing, they looked for shared personality and behavioral traits between offenders and noted current strategies in place used to curb cybercrime and their weaknesses. Their analysis found that while there isn't one set personality that can be applied to all cybercriminals, there were still some common traits that appeared across several studies, including impulsivity, narcissistic tendencies, and high levels of technical ability. The authors note that while there are common traits between some cybercriminals, they depend heavily on variables such as the age of the criminal, background, and the type of cybercrime the offenders engaged in. The authors additionally found that there were several recurring motivations between offenders, including revenge, politics, fame and recognition, curiosity, and financial gain. The

authors' findings help back their claim that cybercrime can't be contained and explained solely by their technological pursuits and that combining understanding of motivation and psychology helps form more effective solutions to the ever-growing cybercrime problem.

One of the most sound connections that can be made between what has been covered in this class and this study is the concept of viewing cybersecurity as both a technological and social science. Time and time again has the idea that cybersecurity needs to be viewed partially as a study of human nature, understanding the behavioral factors that influence individuals to commit cybercrimes or fall victim to them. Another overlapping concept between the article and class is the importance of the use of psychology when studying cybersecurity/cybercrime. The article delves into the motivations, psychological makeup, and personality traits of cybercrime offenders to have a better understanding of why they choose crime and how to prevent their actions in the future. To further connect this study to our class, we learned about how certain personality and psychological traits might contribute to a person's capacity to engage in cybercrime, traits such as narcissism and impulsivity, which the authors of this study specifically mention that many offenders have been found to carry these traits and that while it's not universal, there seemingly is a pattern. Lastly, the article brings up Routine Activity Theory and how this theory, and several more, help explain why cybercrime happens. The idea of this theory is that a crime will only happen when there is a lack of proper guardianship and the presence of a motivated offender; both our class and the article use this idea to reinforce the idea that organizations can use security measures to reduce the opportunities available for a cybercrime to happen.

Unfortunately, the article doesn't make any connection or discuss any challenges, concerns, and/or the contributions of marginalized groups. However, I think some of the topics covered throughout could still be applied when discussing these communities. Individuals who lack technological knowledge, education of security practices, or generally lack digital literacy may be more at risk of falling victim to cybercrimes. These people may not be aware of the most common tactics used in cyberattacks, things like clever social engineering, phishing scams, and malicious links, for example. I also believe that some of the findings from the research on common psychological traits of cybercriminals could be used to help identify those who share those traits and who might be more predisposed to engaging in such cybercrime and who would benefit from education on the topic. I want to stress that the article clearly states that just because an individual might possess these traits, it doesn't necessarily mean they will engage in criminal activities; I was just pointing out that having this knowledge might help lawmakers and cybersecurity professionals discourage cybercrime before it occurs.

I think this study and its authors have made a great contribution to society because the evidence they provided shows that in order to prevent cybercrime, one needs to rely on more than just powerful technology. The research shows that examining the human behaviors and psychological traits that are commonly found among cybercriminals gives cybersecurity professionals, lawmakers, and researchers a much better background and knowledge to allow them to create better prevention

strategies. As cybercrime becomes more common and continues to grow in complexity, incorporating the social sciences, psychology, economics, law, technology, etc, will be necessary to keep up with this ever-advancing climate

Work 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://doi.org/10.5281/zenodo.47661906>