A Psychological Comparison of Online and Offline Criminal Behavior

Ryleigh Holthus
Old Dominion University
06.26.25

Introduction

Psychological motives can drive an individual to commit crime, online or offline, and influence how that criminal behavior manifests. As the world continues to integrate more technology into our everyday lives, the boundary between digital and physical criminality has blurred; however, major psychological distinctions still exist between the two.

This paper explores the question of: How do Online Criminal Behaviors differ Psychologically from Physical-World Crimes?

To answer this question, I examine findings from psychology, criminology, and cybersecurity. Psychology is needed to contextualize the cognitive and emotional frameworks that shape behavior; criminology provides insights into both online and offline crime with broader theories about deviance, opportunity, and social norms. Lastly, Cybersecurity helps us understand how technology enables and alters criminal acts. Looking through these disciplinary lenses allows for a more comprehensive understanding of motivations, deterrents, and behavioral pattern shifts between the virtual and physical world.

An interdisciplinary approach is needed to synthesize findings that no single discipline could fully understand. Psychology explains the *why* behind criminal choices, cybersecurity helps understand the *how* in the digital world, while criminology identifies the societal patterns in both digital and physical environments. The combination of these disciplines supports a more conclusive understanding of criminal behavior, especially since the digital world is becoming increasingly integrated into daily lives. This research is particularly relevant to my major in

cybercrime. My career plans are in digital forensic analysis and my underlying goal of helping others understand target prevention strategies against criminal threats.

Cybercrime, disinhibition, moral disengagement, digital convergence, and *online anonymity* are key terms in my research. Experts in cyberpsychology, McAlaney, Hills, and Cole (2024), define *cybercrime* as illegal behavior facilitated by network technologies and shaped by psychological dynamics in digital environments. *Disinhibition*, as explained by Attrill-Smith and Fullwood (2021), refers to the reduction of social restraint and self-control that occurs in online settings, where anonymity and lack of physical presence reduce concern for consequences (p. 820). Attril-Smith and Fullwood (via Bandura) (2021) also define *moral disengagement* as the process in which individuals justify or minimize the ethical impacts of their actions (harmful or not) (p.820). Defined by Aebi, Miró Llinares, and Caneppele (2025), *Digital convergence* describes the combination of the digital and the physical world interactions, creating a hybrid space where criminal and deviant behavior takes on new forms due to hyperconnectivity and having a broader reach (pp. 93, 106). Finally, Patterson and Winston-Proctor (2019) defines *online anonymity* as the technical and perceptual ability to hide one's identity which is a driving factor in both enabling cybercrime and psychologically distancing oneself from their victims (p.6). These terms build the foundation for understanding how psychological behaviors separate between online and offline criminal contexts.

Psychology

Psychology helps uncover how criminal behavior is influenced by cognitive processes, emotional regulation, and moral reasoning. From a cybercrime perspective, psychological research reveals individuals experience online disinhibition, which leads to higher-risk behavior

and reduced empathy toward victims due to reduced restraint. A fundamental question was raised in the cyberpsychological space by McAnaley, Hills, and Cole (2024): whether people behave differently online or if the technology just enables behaviors that have been suppressed (p.2). The distinction between the two is critical because it challenges the assumption that online criminals are inherently more deviant. Instead, they may feel more free to act without fear of being caught or punished.

Cyberpsychological researchers identify distinct motivations among cyber offenders. Martineau et al. (2023) found that online motivations differ by age group. The youth are more driven by hacktivism, revenge, or plain curiosity. On the other hand, adults lean towards blackmail and behavior linked to mental health conditions. However, across both age groups, dominant motivators are financial gain and entertainment (Section 3.4, para. 3). These findings suggest that cybercrimes are not only driven by a singular mindset but are flexible in psychological incentives which are amplified by the unique environment, the internet.

Martineau et al. (2023) also report that hackers often hold self-centered traits and are not likely to be influenced by family and friends (Section 3.7, para. 2). This aligns with research on moral disengagement, individuals are detached from ethical norms when there is no feedback or direct retaliation from victims, especially online. The emotional distance created by the internet produces a psychological buffer that lowers empathy, which in turn, makes justifying harmful actions easier. Psychology reveals how the virtual world facilitates different methods of crime and different mental conditions for decision-making.

Criminology

Criminology provides insights into how criminal behaviors are shown and brought out within social frameworks and how opportunity, deterrence, and routine activity shape offline and online deviance. Traditional criminological theories were developed based on physical-world crimes; however, many of the core ideas still remain relevant in cyberspace (with minor adaptations to account for the digital environment). Aebi, Miró Llinares, and Caneppele (2025) introduced digital convergence, which is a concept that describes how technological creations have started to blur the boundaries between physical and virtual life, creating a hybrid world (p. 93). In this new hybrid environment, criminal behavior like harassment, fraud, and theft are still fostered, but with a broader reach and fewer geographical limitations. As the authors note, cybercrime is often provoked by hyperconnectedness, which allows offenders to target more victims with great ease (p. 106).

Criminologists have also examined the impact of accessibility in shaping criminal behavior. In routine activity theory, crime occurs when there is a motivated offender, a suitable target, and the presence of no suitable guardian. This theory also applies online where there might be security flaws, user negligence, and weak enforcement. These examples are only a few instances when there is a created space for online crime. Patterson and Winston-Proctor (2019) explain that due to the high value and lack of safeguards, online databases containing financial, medical, and legal information are at the forefront of threats and have become prime targets in cybercrimes. This is unlike the physical world where gaining access to information like data, requires more effort. Protections like physical barriers have caused the digital world to be more appealing. The crime is low effort but has high reward opportunities, not to mention the minimal risk of immediate arrest.

Finally, criminology explores how frameworks (legal and social) adjust or fail to adjust, to ever-evolving criminal acts and tactics. Traditional justice systems struggle to prosecute cybercrime that crosses international borders, lacks physical evidence, and involves pseudonymous identities. This limitation creates offenders who feel as though they are outside the touch of legal consequences. Criminology highlights how outdated law enforcement models and unfamiliar forms of accessibility and convergence contribute to the shift of psychological behaviors in cyberspace.

Cybersecurity

Cybersecurity is another technical field and behavioral lens, it reveals how system designs, digital make-ups, and anonymity influence criminal behavior. Unlike in-person environments, the internet offers tools like encryption, identity masking, and VPNs, that allow users to engage in deviant behaviors without being traced leading to more risk-taking in a lower-risk environment. Patterson and Winston-Proctor (2019) stress the vulnerabilities that online databases hold while storing your personal information, which did not exist in the real world (p. 6). These vulnerabilities heighten crimes in identity theft, doxxing, or even financial fraud. Therefore, expanding the types of individuals that may be made targets.

Cybersecurity experts also explore how system interfaces and user interactions influence moral disengagement. Attrill-Smith and Fullwood (2021) say that user interfaces can be strictly tailored to that user, creating familiarity by mimicking personality traits that influence trust and decision-making (p. 820). When the digital world creates this environment that feels automated and impersonal, users may treat their interactions as disconnected from real-world consequences.

This may lead people to engage in more criminal acts than they would in face-to-face interactions; the detachment from the world may reduce their feelings of empathy and guilt.

Moreover, cybersecurity explores the scale and speed at which cybercrimes can occur. McAlaney, Hills, and Cole (2024) note that the amount of potential offenders is much greater in cyberspace; anyone with basic technical knowledge and internet access is able to participate in harmful acts from anywhere in the world (p. 4). Unlike in the real world, where geographical factors play a huge role in choosing potential victims. Cybersecurity demonstrates the technology that not only facilitates new forms of crime but also how crime has restructured the behavior around criminal acts that shift traditional psychological and criminological thinking.

Common Ground

All three disciplines can agree that anonymity plays a major role in shaping online criminal behavior. Psychology tells us that anonymity lowers empathy and enables disinhibition (Attrill-Smith & Fullwood, 2021). Criminology shows us that anonymity discredits (to some degree) traditional deterrents, making crime more appealing (Aebi et al., 2025). Cybersecurity explains how tools like encryption and identity masking enable offenders to act with little to no fear of consequences (Patterson & Winston-Proctor, 2019).

The disciplines also agree that online environments change emotional and social dynamics. Psychologists report that reduced social feedback online increases impulsivity (McAlaney et al., 2024). Criminology and cybersecurity both support this, showing that crimes often occur in spaces that require less emotional confrontation and weaker protections (Graham & Smith, 2024).

Lastly, each field acknowledges that online crime is fundamentally different from physical crime. Criminology calls for hybrid theories of behavior, while psychology and cybersecurity suggest that online crimes create new psychological patterns and technical risks that need new frameworks.

Disciplinary Conflicts

While the disciplines align on key points of criminal behavior, they diverge when explaining the root causes of cybercrime. Psychology tends to focus on individual cognition, stressing points about impulsivity, self-centeredness, and emotional detachment (Martineau et al, 2023). In contrast, criminology tends to highlight external factors like opportunity structure, weak deterrents, and legal gaps (Aebi et al., 2025). Meanwhile, cybersecurity explains the technical enablers like encryption, digital identity masking, and poor system defenses (Patterson & Winston-Proctor, 2019).

These different conflicts can lead to different interpretations that may clash. For example, psychology may see a cyber criminal as morally disengaged while criminology may see the same act as a rational response to law enforcement. To bridge this gap, there needs to be an integrated approach, one that views behavior as shaped by both internal motivations and external circumstances (including the technological environment that affects certain actions).

Constructing a More Comprehensive Understanding or Theory

By integrating these disciplines, we are able to gain a complete understanding of how online crime behavior is formed. Psychology explains how anonymity and detachment weaken

empathy and increase disinhibition. Criminology highlights how the digital environment decreases possible punishment while amplifying criminal opportunities. Cybersecurity shows us the technology behind these crimes that makes those opportunities possible. Brought together, these insights show that cybercrime is not an extension of offline crime, it is its own category influenced by both internal and external forces.

A new comprehensive theory needs to be developed to understand the interplay between cognitive disinhibition, social opportunity structure, and technical systems. This approach shifts the blame from either the individual or environmental focus. Instead, how digital conditions reshape morals, risk-taking, and deviance need to be considered. Only by connecting these disciplines are we able to fully understand and address cybercrime.

Reflecting on, Testing, and Communicating the Understanding or Theory

The integrated theory or theories can be tested and refined through interdisciplinary research and real-world applications (Repko & Szostak, 2021). For example, future studies may include analyzing data from online personas in contrast to in-person behavior to observe the effects of anonymity on moral disengagement. Cybersecurity analyzers may collaborate with psychologists and see how online behavior alters with system changes. Observing how users behave before and after adding updates to identity verification could help frame the theory of online anonymity. Criminologists could observe how cybercrime rates shift in response to increased digital policing.

These theories require cross-sector cooperation. Law enforcement, digital developers, and policymakers need to understand the psychological and social mechanisms, not just the technical

side of online crime. By applying these findings, institutions can create targeted interventions, therefore reducing the appeal of cybercrime across digital platforms.

Conclusion

This research shows that online criminal behavior differs from offline crime. Not only do methods differ, but the psychological structure as well. Psychology reveals how anonymity and disinhibition reduce empathy and increase disinhibition. Criminology shows that digital environments create lower deterrents and expand opportunities for deviance. Cybersecurity highlights how technology enables and shapes behavior and the crimes committed in suit.

Together, these disciplines emphasize that cybercrime is not only a virtual version of reality, but a distinct form of deviance shaped by its own conditions. Understanding these differences is vital to creating effective prevention strategies, legal frameworks, and digital policies. By taking insights from each discipline, this paper has created a fuller picture of why and how people commit crimes online and why stopping them requires more than just digital solutions.

References

Aebi, M. F., Miró Llinares, F., & Caneppele, S. (2025). *Understanding crime trends in a hybrid society*. Springer Nature.

Attrill-Smith, A., & Fullwood, C. (2021). Disinhibition and moral disengagement in cyberspace. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. Kuss (Eds.), *The Oxford handbook of cyberpsychology* (pp. 816–830). Oxford University Press.

Bandura, A. (1991). Social cognitive theory of moral thought and action. In W. M. Kurtines & J. L. Gewirtz (Eds.), *Handbook of moral behavior and development* (Vol. 1, pp. 45–103). Psychology Press. *(Used indirectly for moral disengagement concept)*

Graham, R., & Smith, K. (2024). *Cybercrime and digital deviance*. Routledge.

Martineau, M., Spiridon, E., & Aiken, M. (2023). A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. *Forensic Sciences, 3*(3), 452–477. https://doi.org/10.3390/forensicsci3030032

McAlaney, J., Hills, P. J., & Cole, T. (2024). *Forensic perspectives on cybercrime: Human behaviour and cybersecurity*. Routledge.

Patterson, W., & Winston-Proctor, C. E. (2019). *Behavioral cybersecurity: Applications of personality psychology and computer science*. CRC Press.

Repko, A. F., & Szostak, R. (2021). *Interdisciplinary research: Process and theory* (4th ed.). SAGE Publications.