Celeste Meraz-Luna

CYSE 201S

Diwakar Yalpi

April 13, 2025

Cybercrime Investigator

Cybercrime investigators rely heavily on social science research and principles, including psychology, sociology, and criminology, to understand offender behavior, assess risk, and engage effectively with marginalized communities. Their work is deeply intertwined with society and shaped by complex human systems.

Introduction

The field of cybersecurity has evolved far beyond technical troubleshooting and code analysis. One critical career path within this field is cybercrime investigation, a profession that combines digital forensics with behavioral science. While technological expertise remains essential, it is social science, particularly psychology, sociology, and criminology, that helps cybercrime investigators understand why people commit cybercrimes, how these crimes affect society, and how to intervene effectively. This paper explores how cybercrime investigators integrate social science principles in their daily work, using concepts from psychology and sociology to address crimes and engage with society, especially marginalized populations who often face disproportionate exposure to online threats.

Social Science Principles in Cybercrime Investigation

Cybercrime investigators consistently apply social science concepts in their routines to decode the “why” behind digital offenses. One of the most relevant frameworks is Psychology and Human Systems Integration, which emphasizes understanding how individuals interact with digital systems. Investigators must assess user behaviors, both lawful and unlawful, to identify threats, build behavioral profiles, and design interventions (Edwards, 2019). For example, phishing attacks exploit human cognitive patterns and emotional triggers, requiring investigators to recognize psychological vulnerabilities when designing countermeasures.

Psychodynamic Theory, developed by Sigmund Freud, also plays a role. This theory posits that unconscious drives, shaped by past experiences, influence behavior. In cybercrime, this can help explain motivations behind cyberstalking, where offenders may be projecting unresolved trauma or social frustration into online actions. Understanding this allows investigators to work with psychologists and legal professionals to build more holistic cases and support rehabilitative approaches for offenders.

Psychological Reactions to Risk are another concept frequently encountered. Investigators assess not just technical vulnerabilities, but human risk perception, how users underestimate or ignore threats. By studying how individuals evaluate digital risks (or fail to), investigators can identify gaps in awareness, particularly among vulnerable groups like the elderly or low-income population who may lack cybersecurity education (Shalaginov et al., 2017).

From a sociological perspective, cybercrime investigators engage with the three main sociological paradigms. Symbolic Interactionism is vital when interpreting online interactions, especially on social media platforms. Understanding the meanings users assign to digital behaviors helps investigators detect threats like cyberbullying or hate speech. Conflict theory is

applied when examining systemic inequalities in digital spaces. For instance, marginalized communities often lack access to protective technologies or face disproportionate targeting by online fraud schemes. Investigators must recognize how structural inequalities shape victimization. Structural functionalism guides policy and law enforcement integration by viewing cybercrime as a disruption to the social order. Investigators work to restore balance by identifying criminal elements and reinforcing norms through education and enforcement (Horan & Saiedian, 2021).

Engaging with Marginalized Groups

Cybercrime investigators play a unique role in protecting marginalized groups who are often disproportionately affected by cyber threats. These groups, including racial minorities and, and those living in poverty, face distinct challenges. Many lack access to cybersecurity education and tools, making them more susceptible to scams and misinformation. Hate crimes, and online harassment often target specific identities. Investigators must understand cultural contexts to build trust and intervene effectively. Some communities are wary of law enforcement, making cooperations difficult. Investigators must use culturally sensitive communication strategies rooted in social science research to build bridges. By applying theories like conflict theory and symbolic interactionism, investigators better understand the social dynamics at play and can advocate for equitable digital protections. This also helps them collaborate with community organizations to educate and support vulnerable populations.

The Cybercrime Investigator and Society

Cybercrime investigators do more than catch criminals, they serve as bridges between evolving technology and societal well-being. Their work influences laws, cybersecurity policy,

and public awareness. As society becomes more digital connected, the demand for socially informed cybersecurity professionals grows. Investigators must balance privacy rights, ethical standards, and justice, reflecting a dynamic relationship between their role and societal norms. Social science offers the tools to understand this complexity and to adapt thier practices as technology and social expectations evolve.

Conclusion

The career of a cybercrime investigator is a prime example of how cybersecurity and social science intersect. Through psychological theories, sociological paradigms, and criminological principles, investigators develop a nuanced understanding of cyber offenders and victims. Their work is deeply informed by concepts such as human systems integration, psychodynamic theory, and social reactions to risk, which help guide daily decisions and broader strategies. Importantly, cybercrime investigators must recognize and address the unique challenges faced by marginalized communities in the digital space, ensuring a more justice and secure society. Their ability to intergrate social science principles into technical work defines thier success in navigating the ever-changing landscape of cyber threats.

References

Edwards, Graeme. *Cybercrime investigators handbook*. John Wiley & Sons, 2019.

Horan, Cecelia, and Hossein Saiedian. "Cyber crime investigation: Landscape, challenges, and future research directions." *Journal of Cybersecurity and Privacy* 1.4 (2021): 580-596.

Shalaginov, Andrii, Jan William Johnsen, and Katrin Franke. "Cyber crime investigations in the era of big data." *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017.