Bridging Cybersecurity and Social Science: Enhancing Digital Forensic Practices

Aaron Cominio

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 24, 2024

BLUF

Digital forensic investigators rely heavily on social science principles to understand human behavior in cyber incidents. By applying concepts like psychological theories, human factors, and cyber victimization, they enhance their work's effectiveness and ethical integrity. Addressing challenges concerning marginalized groups and preserving their relationship with society is essential for maintaining public trust and ensuring equitable practices in the field.

Social Science Principles

Social science principles provide a framework for studying and understanding human behavior, interactions, and social structure. Baranenko et al (2023) identifies the importance of modern science research methods used in investigating cybercrime. Seven key principles include Relativism, Objectivity, Parsimony, Empiricism, Ethical Neutrality, Determinism, and Skepticism. Digital forensics uses these principles to enhance its work's effectiveness, reliability, and ethical integrity.

Relativism is the understanding that all things are related. In a digital forensics context, this principle highlights the need to view cyber incidents not as single events but as part of the larger interconnected societal system. Understanding how socioeconomics influences behavioral decisions helps shape analyses. Investigators who recognize social and systematic interconnections will provide a more holistic evaluation.

Objectivity is a principle that refers to the way scientists approach research in an unbiased manner. Digital forensics investigators must ensure that their analysis and conclusions

are free of biases and based solely on evidence. Objectivity ensures that the findings are credible and can withstand legal scrutiny.

Parsimony calls for simplistic explanations, which is crucial in digital forensics to mitigate overcomplicating findings. Clear, easily understandable communication is required when presenting technical evidence to non-technical audiences, such as police officers or jurors. Simplified explanations ensure a practical understanding of the technical process and findings.

Empiricism is instrumental in digital forensics. This principle relates to investigators only relying on data that can be observed and measured to determine a conclusion. Investigations must be built on factual data. This empirical evidence is the backbone of digital forensic investigations.

Ethical Neutrality requires that all investigators handle data with integrity while abiding by all ethical standards. Given the sensitive nature of gathering digital evidence, this principle is particularly important in digital forensics.

Determinism indicates that preceding events influence behavior. In digital forensics, understanding what events led to a cyber incident is crucial in determining causes and contributing factors. This perspective shapes the investigation by focusing on the actions that led to a cybercrime.

Skepticism is the principle that all assertions should be examined and critically evaluated. This principle applies to digital forensics by requiring the testing and validating of every piece of evidence. This principle mitigates invalid conclusions by ensuring a thorough analysis of all data.

Social science principles provide the foundation of Digital forensic investigations. By actively applying Relativism, Objectivity, Parsimony, Empiricism, Ethical Neutrality, Determinism, and Skepticism, investigators establish an effective, reliable, and ethical framework for their work. Ultimately, integrating these social science principles empowers digital forensic professionals to navigate the complexities of cyber incidents with greater insight and integrity.

Social Science Concepts

Digital forensic investigations incorporate elements of social science. The connection comes from the need to understand the human behavior that contributes to a cyber incident. According to Carley (2020), cybersecurity is about people as social human beings. Social science disciplines such as psychology, sociology, and criminology help investigators understand the behavioral and social factors involved in cybercrime. Cybersecurity as a social science, psychological theories, human factors, and cyber victimization are social science concepts particularly associated with digital forensic investigators.

Digital forensic investigators use the psychological theories of psychodynamic, cognitive, behavioral, and personality to better comprehend the human factors involved in cybercrime. Investigators apply psychodynamic theory to highlight likely actions a cybercriminal might take on their past experiences. Cognitive theory analyzes how an individual thinks and processes information through concepts like neutralization theory. Cyber offenders often rationalize their behavior by denying harm, denying that there was a victim, shifting blame, or claiming their actions were justified. Cyber forensics relies on behavioral theory to understand how cyber criminals learn their behavior, which can help identify correlations and motivations. Finally, personality theories identify key personality traits that investigators use to profile cyber

offenders. These traits are crucial to predict behavior and shape the investigation strategy. Psychological theories are critical for digital forensic investigators to understand cyber criminals' motivations, thought processes, and behaviors, contributing to effective investigations.

Human factors influence technology use, which is highly relevant to digital forensic investigations. Understanding how cyber criminals interact with technology systems provides clues about the cyber offender. Knowledge of human behavior assists with identifying methods a cybercriminal uses to exploit their victims. These behavioral insights also help investigators profile the behavior and habits of the cyber offender. The psychological and human factors provide digital forensic investigators with a broader perspective that is used to develop successful investigations.

Digital forensics relies on cyber victimization to shape the investigation and gather evidence for prosecution. Understanding cyber victimization allows the analysis of victims to help build a criminal profile. Studying the patterns, traits, and behaviors of cyber victims can also help piece together how the cyber incident took place. Identifying how a cybercriminal took advantage of these patterns, traits, and behaviors is used to build a case for prosecution. Cyber victimization is directly tied to digital forensics by guiding investigation approaches and the development of legal evidence.

Digital forensics is a multidisciplinary field that merges technical expertise with social science principles. By incorporating cybersecurity as a social science, psychological theories, human factors, and cyber victimization, digital investigators gain deeper insights into cyber criminals' behaviors and methods. This human-centered lens provides effective and comprehensive strategies for evidence collection and analysis. Social science in digital forensics underscores the essential role human behavior plays in cyber incidents.

Marginalization

The digital forensic investigation career faces several challenges concerning marginalized groups. Research done by Sunde and Dror (2021) highlights the range of possible errors derived from human factors in digital forensics. Diversity, unconscious biases, and economic resources are digital forensics' three most significant challenges. One of the main challenges is the underrepresentation of women and ethnic minorities in digital forensics. This leads to a need for more diverse perspectives in investigative practices. Unconscious bias towards minority groups could unfairly target or overlook certain communities. Data interpretation or profiling may lead to injustice towards marginalized communities. Finally, economic disparities limit individuals in marginalized groups from the digital forensic career. Individuals may need more resources available for education and training opportunities, preventing them from entering the field. Addressing these issues in the digital forensics investigation career is imperative to increase diversity, mitigate biases, and ensure equitable access to resources.

Connection to Society

Digital forensic investigators have a dynamic relationship with society. Deibret (2018) argues that securing human rights is essential to a human-centric approach to cybersecurity. Two complex interactions with digital forensics and society involve balancing security with privacy and public trust. First, balancing security with privacy is a significant challenge for a cyber investigator. Investigations must be conducted in accordance with privacy laws and regulations. Stepping outside of these boundaries creates ethical tensions within society. Secondly, society values personal data protection, so digital forensic professionals must navigate their careers carefully to maintain public trust. Unjust investigations or mishandling of data can lead to the erosion of this trust. Investigations must be transparent and unbiased. Ensuring investigations are

conducted fairly while respecting privacy rights strengthens the relationship between society and digital forensic investigators.

Conclusion

Digital forensic investigation is deeply intertwined with social science principles, shaping the process and outcomes of investigations. The integration of these principles allows investigators to analyze human behavior, interactions, and the social dynamics that contribute to cybercrimes, ensuring that investigations are effective, reliable, and ethically sound. Challenges related to diversity, bias, and economic disparities highlight the importance of fostering inclusivity and fairness within the field to enhance the quality of investigations and represent all segments of society. The balance between safeguarding privacy and maintaining public trust is essential. As society becomes increasingly digital, the role of social science in digital forensics will continue to grow, underscoring the importance of developing strategies that are not only technically sound but also human-focused.

References

Baranenko, D., Koval, A., Dulskyi, O., Lisitsyna, Y., & Musayev, E. (2023). Methodological principles of research in the field of ensuring evidence collection (on the example of cybercrimes): criminal-legal, criminal-procedural, and forensic aspects. *Amazonia Investiga*, *12*(67), 232–240. https://doi.org/10.34069/AI/2023.67.07.21

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, *32*(4), 411–424. https://doi.org/10.1017/S0892679418000618

Sunde, N., & Dror, I. E. (2021). A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making. *Forensic Science International. Digital Investigation (Online)*, *37*, 301175. https://doi.org/10.1016/j.fsidi.2021.301175