Annotated Bibliography

Hailey Caram

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor: Matthew Umphlet

June 29, 2025

Annotated Bibliography

Bennis, M. (2023). Cyber Anthropology and the Construction of Online Identities and Memories: A Theoretical framework. *International Journal of Science and Research (IJSR)*, *12*(3), 1508–1515. https://doi.org/10.21275/sr23325032055

This article discusses the idea of cyber anthropology to study how digital environments are shaping personal identities, memories, and the way people interact within communities. Bennis explains theories such as cybernetics and liquid identities to describe how identities are fluid throughout cyberspace. This is relevant because it is attempting to explain online behaviors (cybersecurity risks) through a social science lens such as anthropology. The article was published in a peer-reviewed journal within the last three years and the hypothesis is reasonably sound. This article contributes to how behavior within online communities can hold up or go against cybersecurity frameworks already in place.

Darabseh, R. S. (2025). The Sociology of Cybercrime: Causes and Prevention. *Pakistan Journal of Life and Social Sciences*, *23*(1). https://doi.org/10.57239/PJLSS-2025-23.1.00318

This study conducted by Darabseh looks at cybercrime from a sociological point of view and identifies both societal and individual causes of criminal cyber acts. Darabseh claims that solutions should stem from education, technological defenses, and collaboration across disciplines. The relevance of this article is high because it directly correlates sociology and cybercrime and discusses how social issues and motivations are fueling criminal activities online. This article was published this year (2025) in a well-known social sciences journal and is supported by substantial research. The importance of this work is within its connections to cybercrime and societal matters.

Rich, M. S., & Aiken, M. P. (2024). An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sciences (Basel, Switzerland)*, *4*(1), 110–151. https://doi.org/10.3390/forensicsci4010008

This article combines cyberpsychology and digital forensics in the Cyber Forensics Behavioral Analysis (CFBA) model, where the goal is to predict try and predict cyber threats through behavioral science. The authors are arguing that the usual cybersecurity methods of relying on technology to secure their systems are not enough to respond to the evolving cyber threats that are driven by human behavior. The study then goes on to offer proactive solutions to the problem. This article is relevant because it is directly using psychology to present a solution to cybersecurity issues. Only being a year old, the article is peer-reviewed and relies on strongly supported theories and methodologies. The significance is evident in its ability to answer cybersecurity problems with an interdisciplinary approach.

Tennakoon, H., Betts, L., Chandrakumara, A., Saridakis, G., & Hand, C. (2024). Exploring the effects of personal and situational factors on cyber aggression. *Cyberpsychology Journal of Psychosocial Research on Cyberspace*, *18*(3). https://doi.org/10.5817/cp2024-3-7

The authors of this article examine how external factors like peer pressure and traits like empathy can predict cyber aggression across social media platforms. The study finds that those with less self-control and anonymity are found to be showing aggressive behaviors in online spaces. This is particularly relevant as it intersects human behavior and potential cybersecurity issues. The article is peer-reviewed and published within the last year. It uses psychological models and substantial research. This study is significant because it offers psychological insights into cybersecurity vulnerabilities.