Social Cybersecurity: An Emerging Science

James F. Keith

CYSE201S: Cybersecurity as a Social Science

Professor Trinity Woodbury

February 21, 2025

Social Cybersecurity: An Emerging Science

Cybersecurity is an interdisciplinary field that integrates multiple disciplines to address cyber-related threats. In her article “Social Cybersecurity: An Emerging Science,” Kathleen M. Carley explores how social science methods can impact cyber-based communications. By combining social science principles like human interaction, group dynamics, and decision-making processes with cybersecurity principles such as cybercrimes, cyberbullying, and misinformation, one can develop a cohesive understanding of the societal impacts posed by these digital threats.

In her research, Kathleen investigated how online narratives, such as misinformation, influenced the public’s perception of societal issues. She hypothesizes that cyber threats are becoming more socialized in nature, which requires behavioral science-driven strategies to counteract them effectively. Questions include “How do online influence campaigns alter the public’s perception?” and “What role does computational social science play in reducing these threats?” Further, the role of emotional triggers in cybercrimes and what can be done to counteract these triggers are inspected.

Kathleen’s study employs computational social science techniques to answer these questions comprehensively. According to the article, “Social cybersecurity uses computational social science techniques to identify, counter, and measure (or assess) the impact of communication objectives. The methods and findings in this area are critical, and advance industry-accepted practices for communication, journalism and marketing research” (p. 2). By analyzing mass social media data and machine learning models to identify and track disinformation campaigns, researchers examine public sentiment to understand how the public reacts and engages with the content. Further investigation shows that the research relies on data from social media posts, reactions, and engagement metrics to assess the spread of disinformation, allowing researchers to develop strategies to counteract it. The analysis of metadata further enables researchers to identify the source of the campaign and ascertain whether bots contribute to the proliferation of posts. Once the source is established, researchers can analyze engagement trends and emotional responses to determine if a specific minority was targeted.

A thorough article analysis reveals key connections to social science and cybersecurity-based concepts discussed in the course. It emphasizes that cybersecurity goes beyond encryption and security measures; it involves recognizing how threat actors exploit social manipulation tactics to uncover vulnerabilities in the public. Specifically, the article highlights how cyber thieves target marginalized groups with disinformation campaigns and harassment. Cyber warfare is a complex issue connected to social and economic factors. Only through understanding these concepts can security professionals effectively combat these attacks.

In conclusion, this study contributes to society by highlighting the importance of taking a more holistic approach to cybersecurity. By incorporating social science and human factor methodologies to combat cyber threats, security professionals and policymakers can design targeted solutions that protect against these threats. The findings confirm that taking an interdisciplinary approach to the problem is the best way to mitigate human-based cyber risks effectively.

References

Carley, K. M. (2020). Social Cybersecurity: An Emerging Science. Computational and Mathematical Organization Theory, 1-17. https://doi.org/10.1007/s10588-020-09322-9