Article Review #2

Private Surveillance and Cybersecurity in the Digital Age

Nadir Harper

CYSE 201S, 28219; Diwakar Yalpi; 9 April, 2025

I. Introduction

Protecting digital environments is a critical function of cybersecurity analysts. Social science heavily impacts the discipline, even if it frequently entails technical duties like network monitoring, vulnerability assessment, and incident response. Ethics, power relations, social norms, and human behavior influence cybersecurity practice. This essay examines how cybersecurity analysts apply social science theories and research, especially when interacting with users, underrepresented groups, and the general public. Social science ideas like ethics, cultural sensitivity, and behavioral psychology are beneficial and necessary for fair and efficient cybersecurity practice.

II. Behavioral Science and Human Factors in Cybersecurity

Understanding human behavior is one of the most significant areas where social science and cybersecurity studies converge. Instead of using technology flaws, many assaults, including phishing, pretexting, or baiting, take advantage of human psychology. To foresee and counter such strategies, cybersecurity analysts employ behavioral science research. Parsons et al. (2015) claim that human mistakes, not system flaws, frequently cause cybersecurity failures. Analysts employ behavioral models to understand user susceptibility and enhance training processes. Social engineering depends on psychologically based cues such as urgency, authority, and trust (Workman, 2008). Analysts with training in these fields can better identify manipulation trends and effectively instruct users.

III. Ethics, Surveillance, and Marginalized Communities

Monitoring and gaining access to private information is standard in cybersecurity operations. This duty necessitates a solid ethical basis, particularly for those employed in government, healthcare, or education, where underprivileged groups may already experience social injustices. According to van den Hoven et al. (2020), cybersecurity design and decision-making must incorporate ethical thinking. Analysts often encounter problems with user privacy, consent, and fairness. Furthermore, studies indicate that monitoring technologies may disproportionately target or damage vulnerable people if uncontrolled (Eubanks, 2018). A socially aware cybersecurity analyst evaluates whether procedures or technologies might perpetuate systemic prejudices using social science frameworks like intersectionality and structural inequality. Analysts aware of these dynamics can influence more equitable cybersecurity regulations and push for more comprehensive data protection.

IV. Communication, Training, and Cultural Competence

Cybersecurity Analysts are also responsible for communicating risks and recommended practices to non-technical people. Social awareness and cultural competency are necessary for this. Bada, Sasse, and Nurse (2019) claim that ignoring organizational, social, and cultural settings frequently fails awareness initiatives. Social science research sheds light on how various populations use digital information, engage with authorities, and perceive risk. For example, historical prejudice or restricted access to resources may cause disadvantaged populations to distrust institutional communications. By comprehending these dynamics, analysts may modify communication tactics and improve cybersecurity's usability and accessibility for all users. Analysts also frequently collaborate with international stakeholders or in varied teams. Social

science training enables students to collaborate and negotiate cultural differences, two abilities that are becoming increasingly crucial in today's networked digital environment.

V. Conclusion

Cybersecurity analysts are social communicators, ethical decision-makers, behavioral strategists, and technological specialists. Their work relies on communication theory, psychology, sociology, and ethics. By utilizing social science, they may better safeguard users, prevent harm to vulnerable groups, and advance equity and inclusivity in digital environments. The need to incorporate social science into cybersecurity analysis will only increase as cyber threats change to protect systems and serve society morally and fairly responsibly.

References

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672. https://arxiv.org/abs/1901.02672

Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor—St Martin's Press.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2015). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 48, 42–57. https://doi.org/10.1016/j.cose.2014.10.003

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2020). Privacy and information ethics. In The Cambridge Handbook of Information and Computer Ethics. Cambridge University Press. https://doi.org/10.1017/9781139018459

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretextual social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779

National Institute of Standards and Technology (NIST). (2020). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

https://csrc.nist.gov/publications