Cybersecurity Professional Career Paper: Cyber Defense

Nathan Jimenez

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

11/14/2025

Introduction

Cybersecurity is one of the fastest growing professions in the world, it is responsible for protecting digital systems, sensitive information, and critical infrastructure from attacks. As we move to a more technology dependent world we will depend on it more than we are now for communication, finance, healthcare, education, and national security, the importance of cybersecurity continues to grow. Cyber defense plays a central role in identifying threats, preventing intrusions, and responding to incidents. The purpose of this paper is to explore how cyber defense careers rely on social science principles and how key concepts from class apply to this profession. It also will talk about how cybersecurity impacts marginalized groups and how cyber contributes to society.

Social Science Principles and Their Relation to Cyber Defense

Social science research is essential in cyber defense as many cybersecurity threats are rooted in human behavior. Cyber defense analysts must understand why people engage in such risky online behavior and how attackers manipulate human psychology, and how organizational culture influences digital safety. A core social science topic in cybersecurity is hacking motivation. Research shows that hackers often act for financial gain, curiosity, or revenge. By understanding these motives it helps cyber defenders anticipate attack patterns and design effective preventative measures. Professionals also use social science insights to develop cybersecurity awareness strategies, such as teaching employees how attacks use pretexting, deception, trust manipulation, and authority pressure in phishing emails.

Application of Key Concepts

The cyber defense career heavily uses key concepts such as the CIA Triad, risk Assessment, Vulnerability Management, and Incident Response. These play a big part in every daily task that cyber defenders perform. An example would be that defenders apply the CIA Triad when evaluating incidents or setting up controls. They use risk assessment tools to measure the likelihood and impact of attacks. Defenders also implement protocols based on principles like deterrence, accountability, and transparency.

Marginalization in the Context of Cyber Defense

Cybersecurity doesn't impact all groups equally. Marginalized groups often experience unequal digital protection due to the limited access to secure technology, lower digital literacy, or fewer resources to recover from identity theft or financial fraud. Cyber defense professionals work to address these disparities by promoting digital safety, supporting outreach programs, and encouraging diversity in cybersecurity hiring. Additionally, policies around privacy, surveillance, and data protection must consider how marginalized groups are disproportionately monitored or exploited online

Career Connection to Society

Cyber defense professionals contribute directly to the safety, stability, and functioning of modern society. They protect essential infrastructures such as hospitals, financial institutions, schools, transportation systems, and government networks. Without cyber defense, ransomware, service outages, and data breaches would disrupt daily life and threaten economic stability. Cyber defense also intersects with public policy. Laws such as the Cybersecurity Information

Sharing Act (CISA) and international cyber treaties reflect society's increasing need for coordinated digital protection.

Scholarly Journal Articles

Source 1:

Greitzer & Frincke (2010) highlighted how psychological and social indicators help predict insider threats. Their research is relevant to cyber defense because it shows that it is not only technical.

Source 2:

Yar & Steinmetz (2019) explore cybercrime motivations, social influences, and digital deviance. This supports the idea that understanding social science principles is essential for analyzing attacker behavior and designing preventative measures.

Source 3:

Reisach (2021) discussed global cybersecurity inequities and how marginalized groups face disproportionate risks. The article connects directly to the section on marginalization and demonstrates the societal impact of cyber defense work.

Conclusion

Cyber defense is a complex profession as it requires a combination of technical skills and social science knowledge. Understanding human behavior, motivation, ethics, organizational culture, and social inequalities helps cyber defenders create stronger security systems and respond fast to threats. This profession is essential in today's world, and its connection to social science makes it more effective, inclusive, and responsive to the needs of all communities.

References

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. Insider Threats in Cyber Security, 85–113. https://link.springer.com/chapter/10.1007/978-1-4419-7133-3_5

Reisach, U. (2021). The responsibility of social media companies for digital communication and cyber risks. Journal of Cybersecurity, 7(1). https://academic.oup.com/cybersecurity/article/7/1/tyab003/6248895

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (3rd ed.). SAGE Publications.