**Cybersecurity Professional Career Paper: Title of the paper**

Student Name: Eric Zhao

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/16/2025

## Introduction

Cybersecurity has become one of the most critical professions of the 21st century as societies increasingly rely on digital technologies to support economic activity, healthcare, finance, education, and government operations. Within this broad field, Security Operations Center (SOC) analysts serve on the front lines of digital defense. They monitor networks, investigate suspicious activity, and respond to cyber incidents that threaten organizational stability. In a world where cyberattacks grow more sophisticated and frequent, SOC analysts are essential to maintaining trust in digital infrastructures and safeguarding sensitive information.

The purpose of this paper is to explore the profession of SOC analysts through a multidisciplinary lens. It examines how social science principles shape cybersecurity practices, how key concepts apply to real-world SOC work, how cybersecurity intersects with marginalization, and how the profession contributes to societal stability. Finally, the paper reviews scholarly journal articles that provide empirical evidence and insights into the SOC analyst role.

## Social science principles

Social science offers valuable frameworks for understanding the human behaviors that influence cybersecurity—both from the perspective of attackers and users. For example, criminological theories help explain motivations behind hacking, whether financial gain, political ideology, thrill-seeking, or social recognition. These insights give SOC analysts context when analyzing threat patterns or responding to incidents.

Social science principles also influence how analysts interpret human-computer interaction (HCI) and user behavior. Many cyber incidents stem from predictable human tendencies such as trust, error, cognitive overload, or misunderstanding of security protocols. SOC analysts often investigate phishing attacks, misconfigurations, and insider threats—issues grounded as much in psychology and sociology as in technology.

Professionals apply these principles in training and awareness programs. For example, understanding social engineering tactics rooted in persuasion theory enables analysts to help develop realistic phishing simulations or educational campaigns. This mix of behavioral science and technical defense makes cybersecurity more holistic and effective.

## Application of Key Concepts

Cost-benefit analysis (CBA) is a critical concept for SOC analysts as they balance security needs with organizational constraints. In their role, analysts continually weigh the cost of time, tools, and resources against the benefit of reducing risk, improving detection, and maintaining compliance. This applies to prioritizing alerts, recommending security tools, evaluating security controls, and supporting risk assessments. SOC analysts also use CBA to justify implementations that strengthen security posture while avoiding unnecessary spending, ensuring that controls not only enhance protection but also meet regulatory and legal standards.

The application of CBA is supported by tools and methodologies that help quantify risk and measure the value of security actions. SIEM platforms like Splunk or Microsoft Sentinel provide incident data that inform cost-impact decisions, while models such as FAIR and CVSS help prioritize vulnerabilities based on potential organizational harm. Technologies such as threat intelligence platforms, SOAR automation, and incident response metrics (MTTD/MTTR) further allow analysts to assess whether improvements justify their financial and operational costs. Through these tools and techniques, SOC analysts apply cost-benefit analysis to guide effective, informed, and economically sound cybersecurity decisions.

## Marginalization

Cybersecurity has unequal effects on marginalized groups. Communities with limited access to technology, technical education, or economic resources often face greater vulnerability to cyber threats such as fraud, identity theft, or exploitative surveillance. Additionally, marginalized populations may be disproportionately targeted in cyberattacks, especially in the context of political disinformation or financial scams.

The cybersecurity profession—including SOC roles—has begun acknowledging these inequalities. Initiatives to diversify the workforce, expand STEM access, and promote digital equity aim to ensure that cybersecurity protections benefit all groups. Ethical guidelines and privacy-focused policies also help protect marginalized communities from intrusive data practices. By broadening participation and advocating for equitable protections, SOC analysts can contribute to reducing digital disparities.

## Career Connection to Society

SOC analysts play a crucial role in protecting digital systems that support everyday life. They defend financial networks from fraud, ensure hospitals remain operational during attacks, and safeguard government systems that manage public services. These contributions directly affect societal stability and the public's trust in essential institutions.

Public policy also shapes the SOC profession. Laws related to data protection, breach reporting, and critical infrastructure security determine what organizations must monitor and how they must respond to incidents. SOC analysts help organizations comply with these regulations by maintaining logs, preserving evidence, reporting intrusions, and implementing protections aligned with national cybersecurity standards. Their work therefore operates at the intersection of technology, governance, and societal well-being.

## Scholarly Journal Articles

Source 1: "A systematic method for measuring the performance of a cyber security operations centre analyst" (Computers & Security, 2023).
This study proposes a structured framework for evaluating SOC analyst performance, addressing a long-standing gap in consistent assessment. The article is relevant because it demonstrates how SOC roles require both technical expertise and decision-making skills

informed by human-factor considerations, supporting the discussion of key concepts and professional responsibilities.

Source 2: “SAIBERSOC: Synthetic Attack Injection to Benchmark and Evaluate the Performance of Security Operation Centers” (ACM, 2020).
This research introduces a method for injecting realistic attack simulations into SOC environments to measure analyst responses. It supports the paper’s analysis of social science principles because it highlights human behavior under pressure—how analysts detect, interpret, and respond to simulated attacks, revealing cognitive patterns and decision-making strategies.

Source 3: “Technical performance metrics of a security operations center” (Computers & Security, 2023).
This article contributes to understanding how SOC analysts connect to broader societal needs. By defining performance metrics for detecting and mitigating threats, the study illustrates how SOC functions directly influence organizational resilience and societal infrastructures. It also reinforces the paper’s discussion of applied cybersecurity concepts and compliance-driven operations.

## Works Cited

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2023). A systematic method for measuring the performance of a cyber security operations centre analyst. Computers & Security, 124, 102959. https://doi.org/10.1016/j.cose.2022.102959

Forsberg, J., & Frantti, T. (2023). Technical performance metrics of a security operations center. Computers & Security, 135, 103529. https://doi.org/10.1016/j.cose.2023.103529

Rosso, M., Campobasso, M., Ganduulga Gankhuyag, & Luca Allodi. (2020). SAIBERSOC: Synthetic Attack Injection to Benchmark and Evaluate the Performance of Security Operation Centers. Annual Computer Security Applications Conference. https://doi.org/10.48550/arXiv.2010.08453