# Cybersecurity Professional Career Paper: Cyber Intelligence Analyst

Tyler Walker

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 16, 2025

## Introduction

A Cyber Intelligence Analyst is one of the most important roles in modern cybersecurity because these professionals track threats, study attacker behavior, and help organizations stay ahead of cybercriminals. As cyber threats grow more complex, understanding technology alone isn't enough, analysts also need to understand people. The purpose of this paper is to explain how Cyber Intelligence Analysts rely on social science principles every day, how class concepts from CYSE 201S apply to their work, how the career affects marginalized groups, and how this field connects to society as a whole.

## Social Science Principles in the Career

A big part of cyber intelligence work is understanding why people behave the way they do online, which ties directly into the social science ideas from Module 2. Cyber Intelligence Analysts have to stay objective when reviewing threat information, which means they can't rely on gut feelings or jump to conclusions about an attacker. Instead, they depend on evidence from threat reports, communication trails, and digital activity, which reflects the social science principle of empiricism. Determinism also shows up in this career because cyberattacks don't just happen at random. They're driven by motives like money, ideology, group identity, and even larger political trends. Module 3's focus on research methods connects well here too, since analysts basically act like social science researchers. They gather data, categorize indicators, compare patterns, and study how hacker communities operate. These online spaces often have their own culture, hierarchy, and rules that shape how attackers act. Shakarian (2017) supports this idea by

explaining that defenders make smarter decisions when they understand the voices, motivations, and communication patterns of their adversaries.

## Application of Key Course Concepts

A lot of what we learned in CYSE 201S shows up almost naturally in the everyday work of a Cyber Intelligence Analyst. For example, Module 5 goes over concepts like cognitive theory, behavioral theory, personality traits, etc., these theories help analysts get a better understanding of why attackers behave the way they do. Cognitive theory, for example, explains how some attackers justify their actions or convince themselves that the damage they cause isn't a big deal. Behavioral theory fits too, because many cybercriminals pick up their techniques, habits, and even their "hacker identity" from the online groups they hang around in. Module 6's focus on human factors and risk perception shows up when analysts study why certain people fall for phishing or why attackers choose specific targets. Module 12 takes things a step further by breaking down motives, whether someone is driven by money, ideology, revenge, or just trying to gain status online. These motives help analysts piece together who the threat actor might be. Shakarian (2017) reinforces this entire approach by explaining that good intelligence work is about understanding the attacker's mindset, culture, and communication style so defenders can stay one step ahead.

## Marginalization and Ethical Considerations

Cyber Intelligence Analysts must also consider how cyber threats and cybersecurity practices impact marginalized groups. Module 12 explains that certain groups, such as low-income populations, minorities, the elderly, and individuals with

limited digital literacy, are more vulnerable to cyberattacks. Analysts must consider these disparities when recommending security strategies. There are also ethical challenges, such as avoiding algorithmic bias and ensuring fair analysis. Diversity in the cybersecurity workforce improves intelligence accuracy and supports equitable digital protection.

## Career Connection to Society

Cyber Intelligence Analysts contribute directly to society by helping protect major systems such as healthcare networks, financial institutions, government agencies, and communication infrastructures. Their intelligence reports inform public policy, guide national security decisions, and help organizations prepare for emerging threats. Shakarian (2017) shows that smart cyber defense depends on understanding societal risks, attacker objectives, and geopolitical tensions, proving that cyber intelligence is deeply connected to society.

## Scholarly Journal Insights

Shakarian (2017) argues that high-quality threat intelligence relies on understanding attacker communities, motivations, and communication patterns. This shows how analysts depend on social science to interpret human behavior behind cyber threats. Holt and Bossler (2016) explain how routine activity theory helps analysts understand attacker decisions, while Hutchings and Clayton (2016) highlight how online criminal forums shape hacker norms and behaviors.

## Conclusion

In conclusion, the role of a Cyber Intelligence Analyst is deeply connected to the social sciences. Analysts use concepts such as objectivity, empiricism, behavioral theory, cognitive theory, and research methods from CYSE 201S to study the people behind cyber threats. The career also requires an understanding of how cybercrime affects marginalized groups and how intelligence work protects society as a whole. By blending technical skills with social science principles, Cyber Intelligence Analysts help organizations make smarter decisions, respond to threats more effectively, and build a safer digital world.

## References


Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436. https://doi.org/10.1177/1043986213507401 (Original work published 2013)

Hutchings, A., & Clayton, R. (2016). Exploring the role of online forums in cybercrime. European Journal on Criminal Policy and Research. https://arxiv.org/html/2208.10629v6

SHAKARIAN, P. (2017). THREAT INTELLIGENCE VS. THE "OFFENSE DOMINANT" CYBER PARADIGM. In *THE ENEMY HAS A VOICE: Understanding Threats to Inform Smart Investment in Cyber Defense* (pp. 3–7). New America. http://www.jstor.org/stable/resrep10515.4

SHAKARIAN, P. (2017). Understanding Proactive Cyber Threat Intelligence Methodology. In *THE ENEMY HAS A VOICE: Understanding Threats to Inform Smart Investment in Cyber Defense* (pp. 7–8). New America. http://www.jstor.org/stable/resrep10515.5