Cybersecurity Professional Career Paper: Cyber Threat Intelligence Analysts and Social Science Principles

Christopher Rojas

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

11/13/2025

Introduction

The cybersecurity profession is a specialized field in computer technology that focuses on an essential part of technology that is security. In today's age of technology, it is of utmost importance to protect and secure our data from potential threat actors. The purpose of this paper is to highlight a crucial role in the cybersecurity field: Cyber Threat Intelligence Analyst. The primary focus will be how this role relates to social science, marginalized groups, and society.

Social science principles

Cyber Threat Intelligence Analysts utilize a wide variety of social science principles in order to do their job. Their primary focus is people and the motivations behind cybercrime; by using psychology (and other technical methods) they attempt to foresee cyber-attacks before they even occur. CTI analysts attempt to find patterns in behaviors displayed online through data feeds (i.e. forums, malware, dark web). For example, theories of social learning can help analysts implement anti-phishing campaigns based on behavioral patterns. "Human error remains a consistent and significant threat. Threat intelligence helps tailor training and awareness programs to counter social engineering tactics and phishing schemes based on trending attack patterns." (Pmmi, 2025)

Application of Key Concepts

Several concepts from class apply to cyber threat intelligence analysts. CIT analysts conduct field research as a complete observer to gain insight on how threat actors might plan or conduct cybercrime. Their objective is to gather as much data as possible to prevent attacks. Behavioral theories and cyber-criminal subculture are also taken into consideration by CIT analysts often scouting forums to identify peer networks that engage in cyber offending. Lastly, a security protocol implemented through environmental design from CIT analysts are honeypots. For example, Honeypsy was designed to observe behavior by using machine learning algorithms to spot unusual behavior and therefore better protect organizations (Saeed, Suayyid, Al-Ghamdi, Al-Muhaisen, Almuhaideb, 2023)

Marginalization

Challenges arise that clash with CIT roles and marginalized groups. Minorities might not have a clear pathway to pursue a CIT role, especially when no one in the person's peer network is involved in cybersecurity. CIT roles involve the combating of crime, which can lead to certain prejudices leaking over from law enforcement. Certain groups might even be targeted for surveillance due to their ethnic background. Unequal pay is also a concerning issue in cybersecurity that could affect minorities in CIT roles "a cybersecurity professional of color earns $115,000, while the overall U.S. cybersecurity workforce average is $122,000" (ISC, 2018). The cybersecurity field is also attempting to address these challenges. Non-profits such as Consortium of Minority Cybersecurity Professionals aim to create opportunities for these marginalized groups to receive scholarships to pursue cybersecurity careers.

Career Connection to Society

CIT analysts contribute to the safety of several societal structures, although disproportionately to their rate of industry adoption "CTI is used in very few sectors of the industry (notably banking and finance, government, and technology" (Ainslie, 2023) Their knowledge and ability predict future attacks brings a previously not seen layer of safety in the cybersecurity field. Public policies relate to CIT analysts in a major way. When trying to predict future behavior, a level of speculation is utilized to gain foresight. Although machine learning detection and behavioral theories are grounded methods of understanding potential cyber-criminal behavior, it is also dangerous to engage in invasions of privacy and assumption. By creating policies such as breach notification laws and privacy protections, CTI analyst roles can protect organizations while respecting civil liberties.

Scholarly Journal Articles

Cybersecurity Threat Intelligence – Should I have one? (2025). Pmmi.org. https://www.pmmi.org/blog/cybersecurity-threat-intelligence-should-i-have-one?

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. mdpi. https://doi.org/10.3390/s23167273

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, *132*(132), 103352. https://doi.org/10.1016/j.cose.2023.103352

ISC)2. (2018, March 15). *(ISC)2 Study Finds U.S. Minority Cybersecurity Professionals Underrepresented in Senior Roles*. Prnewswire.com; Cision PR Newswire. https://www.prnewswire.com/news-releases/isc2-study-finds-us-minority-cybersecurity-professionals-underrepresented-in-senior-roles-300613320.html