Cybersecurity Professional Career Paper: Cyber Threat Intelligence Analyst

Student Name: Hans Joshua P. Sawi

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Diwakar Yalpi

Date: 04/14/2026

Hans Joshua P. Sawi 04/14/2026

Introduction

A Cyber Threat Intelligence Analyst researches cyber threats and assists organizations in comprehending the individuals who might attack, the reasons why they might attack and the methods of attack. The significance of this role is that contemporary life is based on digital systems in the banking sector, healthcare, education, business, and government. Cybersecurity is perceived as a technical discipline. However, it relies on social systems and human behaviors as well as decision-making. That is why social science can be of much help in this profession. It requires that a Cyber Threat Intelligence Analyst is not only familiar with malware and network threats, but also human motives, patterns of communication, and risk behavior. This paper describes the links between social science concepts and this career, the importance of major concepts in the job, and the impact of cybersecurity on marginalized groups, as well as how the occupation relates to society.

Social science principles

Social science studies play a significant role in cybersecurity, as a lot of cybercrimes involve human activity. Individuals can follow phishing links, use weak passwords, disregard warning messages, and provide sensitive data without considering the probability of an attack. Meanwhile, the motives, beliefs, social pressure, and learned behavior also guide attackers. Studies indicate that attitudes, social norms, self-control, and perceived risk are the factors influencing cybersecurity behavior, which makes social science handy in understanding victims and perpetrators (Schaltegger et al., 2025). This implies that threat analysis as a Cyber Threat Intelligence Analyst cannot be technology-focused. The analyst should also research the reasons why attackers select specific targets and their motives. Human factor research indicates that the

interaction of technology, behavior, and organizational culture is likely to cause cybersecurity issues, not the technical weakness (Khadka et al., 2025). This is based on the principles of social science, including empiricism and objectivity, as the analysts have to rely on facts, observations, and trends instead of assumptions. Another application of social science is in designing security awareness programs in organizations. The threat intelligence analyst can assist in clarifying the existing scams, discovering frequent emotional appeals in phishing messages, and proposing improved user education. Research on behavioral cyber risks demonstrates that risk communication and specific interventions are more effective when considering the way people think and behave in the real world (Pugnetti et al., 2024). This demonstrates that social science is directly integrated into the practice of cybersecurity.

Application of Key Concepts

A number of social science concepts from the class are relevant to the job of a Cyber Threat Intelligence Analyst. Attacker motivation is one of the key concepts. Attackers can be motivated by money, retaliation, ideology, status or curiosity. Knowledge of these motives assists analysts in estimating probable targets and techniques of attack. Research on cyber threat intelligence reveals that successful intelligence requires research on not only technical indicators, but also the threat actors, their behavioral patterns, and the broader social and organizational context of attacks (Santos et al., 2025). The other useful concept is that of cognition, or the way in which individuals think and make decisions. Both attackers and defenders apply shortcuts in thinking, and they can pose a threat. As an illustration, employees might be too trusting of urgent messages or not be suspicious of unusual requests. Analysts can apply this knowledge to evaluate weaknesses in organizations and enhance warning mechanisms. This is an expression of skepticism, in that the analyst must doubt what he sees on the surface, and parsimony, in that

intricate threats need to be articulated in an understandable manner to the decision-makers. Cyber offending theories in the social sciences are also helpful. The cognitive and behavioral concepts are particularly applicable since they are concerned with learned behavior, rational decisions and repetitions. Practically, these concepts are applied by analysts in evaluating insider threats, spamming, and internet scams. By doing so, the concepts of social science can assist analysts in evaluating the risk, assisting with the security measures, and recommending that the leaders take more to prevent it.

Marginalization

The issue of cybersecurity has a significant impact on marginalized communities. Individuals who have less access to the digital environment, less digital literacy, language obstacles, or less money tend to be more vulnerable to cyber risks. They can be more vulnerable to fraud, identity theft, misinformation or malicious surveillance. Meanwhile, they might lack means of self-protection. Digital exclusion research indicates that disadvantaged communities are influenced by the lack of access to digital resources, digital skills, and assistance, which make them more susceptible in the digital realm (Hollimon et al., 2025). This is important to a Cyber Threat Intelligence Analyst because not all groups are impacted by the threat trends. Analysts need to think about the target audience and the purpose of targeting. The study of AI and cybersecurity also indicates that cyber harm can be used to exacerbate pre-existing inequality, particularly in cases when attacks target healthcare, education, employment, or other areas of state services that already hold great significance to vulnerable populations (Vulpe & Stirbu, 2024).

Hans Joshua P. Sawi 04/14/2026

Career Connection to Society

One of the benefits of a Cyber Threat Intelligence Analyst to society is that they help to keep critical system trusted and safe. Effective cyber threat intelligence helps in ensuring the safety of hospitals, power systems, transportation, financial institutions, and government networks. Earlier detection of probable threats by the analysts will enable organizations to be better prepared and limit damage. This helps in bringing about stability in society, and not merely in a single firm or agency. The position is also related to the policy. Cyber threat intelligence is becoming increasingly important in influencing governments and institutions' security planning, compliance, and incident response. As cyber threats are not only a problem of technology, but also of community life, analysts assist decision-makers in comprehending risk in a manner that contributes to broader resilience. This renders the job to be socially significant as it safeguards both the infrastructure and human beings. Cybersecurity is not only a technical role in this sense. It is also a social duty that is influenced by action, morals and influence.

Conclusion

A Cyber Threat Intelligence Analyst relies on social science in numerous aspects. The position needs an awareness of human behavior, attackers' motives, organizational culture and vulnerable population. The concepts of social science, including empiricism, objectivity, skepticism, and behavioral analysis, assist analysts in making superior judgments and developing resilient security reactions. The concepts are utilized in risk management, threat assessment, user education and compliance. The profession is also highly social in that cybersecurity has an impact on marginalized groups and safeguards critical systems on which people rely. All in all, this profession demonstrates that cybersecurity is not all about machines and code. It is also related to people, their behavior and society as a whole.

References

Hollimon, L. A., Bervell, B., Alhassan, M. D., & Armah, R. A. (2025). Redefining and solving the digital divide and exclusion to advance digital health equity. *Frontiers in Digital Health, 7*, Article 1508686. https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2025.1508686/full

Khadka, K., Williams, M., Nation, J., Barlow, J., & Evans, M. (2025). Human factors in cybersecurity: An interdisciplinary review. *International Journal of Information Security*. https://link.springer.com/article/10.1007/s10207-025-01032-0

Pugnetti, C., Bertolotti, I., Benczur, P., & Tessone, C. J. (2024). Towards diagnosing and mitigating behavioral cyber risks. *Risks, 12*(7), 116. https://www.mdpi.com/2227-9091/12/7/116

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors, 25*(14), 4272. https://www.mdpi.com/1424-8220/25/14/4272

Schaltegger, T., Bearth, A., & Siegrist, M. (2025). Human behavior in cybersecurity: An opportunity for risk research. *Journal of Risk Research*. https://www.tandfonline.com/doi/full/10.1080/13669877.2025.2539109

Vulpe, S. N., & Stirbu, O. C. (2024). AI and cybersecurity: A risk society perspective. *Frontiers in Computer Science, 6*, Article 1462250. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1462250/full