Cybersecurity Professional Career Paper: Network Engineering as a Social Architect

Student Name: Patrick Bays

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/14/2026

Introduction

BLUF: A Network Engineer is no longer just a builder of connectivity, but a foundational defender whose role requires a deep understanding of both technical aspects of networking and human behavior/social science principles to secure critical infrastructure.

Cybersecurity, as a general profession, has evolved from a niche technical field into a multi-disciplinary pillar of global stability. As organizations face increasingly sophisticated threats, a Network Engineer serves as the primary architect of secure perimeters that protect data and privacy. This paper explores how Network Engineering as a career integrates technical expertise with social science to address human vulnerabilities, marginalization, and the safety of societal infrastructures.

Social science principles

Network Engineering relies heavily on understanding human behavior to mitigate risk. Technical aspects like firewalls, port security, etc. are essential, but social science research demonstrates that social engineering remains a primary vector of attack for data breaches. Professionals in this field use human-computer interaction (HCI) principles to design network interfaces and access controls that can guide users toward secure choices without sacrificing productivity or existing work habits. By analyzing user behavioral patterns, Network Engineers can distinguish between routine traffic and anomalous behavior associated with compromised accounts. Strategies for cybersecurity awareness often leverage behavioral psychology to hopefully bypass simple ‘human error’ narratives, and instead incentivize secure habits through intuitive design and clear, layman-readable organizational policies.

Application of Key Concepts

Four concepts from the course modules are directly applicable to a Network Engineer’s daily responsibilities. The concepts are Routine Activity Theory, Rational Choice Theory, Neutralization Theory, and Social Bond Theory.

Routine Activity Theory suggests that crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge. A Network Engineer acts as the ‘capable guardian’ in this instance, by implementing intrusion prevention/detection systems and segmenting networks to ensure that suitable targets (sensitive data) are shielded from said motivated offenders.

Rational Choice Theory proposes that offenders perform a cost-benefit analysis before acting. Network Engineers apply this theory by increasing the ‘cost’ of an attack through technologies like multi-factor authentication (MFA) and rigorous encryption standards, making the effort and risk outweigh the potential reward or benefit for the attacker.

Neutralization Theory explains how individuals justify violating rules. In a professional setting, an engineer might identify an insider threat who justifies bypassing security protocols in the name of ‘efficiency’. Through understanding these psychological justifications, engineers can either implement technical controls that leave no room for bypassing a control, or adapt control implementation/user training such that abiding by the control can be seen as the efficient choice.

Social Bond Theory posits that strong social bonds to an organization (attachment, commitment, involvement, and belief) reduce the likelihood of overall deviance. Network Engineers can support this by maintaining reliable and transparent systems that foster trust between the broader workforce and IT infrastructure/teams, reinforcing the belief in the security mission.

Marginalization

Cybersecurity and network architecture have profound effects on marginalized groups. The ‘digital divide’ often means that marginalized communities have unequal access to secure, high-speed infrastructure that is required for modern participation in society. These groups are also often

disproportionately targeted in data breaches or subjected to higher levels of surveillance. Network Engineers can contribute to addressing these challenges by advocating for equal digital protection policies and working towards initiatives that diversify the field. Helping to ensure that security protocols are inclusive and do not unfairly flag or exclude users based on demographic/cultural variables is also a critical component of modern network ethics and professional responsibility.

Career Connection to Society

Network Engineers are essential to the safety and stability of societal infrastructure, including financial systems, healthcare networks, government operations, and even just organizational operations. A failure in a given network can lead to cascading societal disruptions, such as the inability to process payments or access medical records. Consequently, public policies like the NIST Cybersecurity Framework and CMMC standards guide this profession, ensuring that technical configurations align with broader societal needs for privacy, reliability, accessibility, and national security.

Scholarly Journal Articles

Source 1: Kigerl, A. (2011). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470–486. https://doi.org/10.1177/0894439311422689

This article explores the application of Routine Activity Theory in the digital realm. The findings suggest that technical guardianship (like the guardianship provided by Network Engineers) is effective, but must be combined with social guardianship (user awareness). This supports my paper's argument that engineers must be 'capable guardians' of network perimeters.

Source 2: Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of Employee Information Systems Security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

This study examines how employees use neutralization techniques to justify security policy violations. It supports the analysis of insider threats by showing that technical controls must account for the psychological justifications users (albeit misguidedly) use when bypassing network security protocol.

Source 3: Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1–20. https://doi.org/10.25300/misq/2013/37.1.01

This article combines Social Bond Theory with Neutralization Theory to understand employee behavior. It contributes to the understanding of career connections to society by illustrating how organizational commitment and professional ethics (alongside secure network design) prevent computer abuse that can threaten societal infrastructure.