Cybersecurity is a vast field filled with different specialties and career paths. With proper training and education, you can become a Cybersecurity Analyst, Penetration Tester, Security Operations Analyst or even a Network Engineer. Upon graduating with my bachelor's degree, it is my goal to become a Network Engineer. I would like to use the knowledge that I have gained during my time spent in college to help excel in this career path while gaining new skills. The career path that I am choosing to write this paper on would be Network Engineering. Network engineering is a very detail-oriented career and their daily job duties must be approached tactfully to avoid any major mishaps that could effect the organization from both an ethical and financial standpoint.

Ethical Neutrality is a principle that relates closely to network engineering because network engineers must adhere to certain standards to protect the organization. A question that a social scientist my address in this field would be "How can we protect sensitive information while safeguarding the network from vulnerabilities". Network engineers work closely with data privacy, and it is important that they make ethical decisions to help protect the organization. This career path is very attention-to-detail oriented and if they aren't careful both personal regarding the employees within the organization and sensitive information could be leaked which would cause a major and potentially costly issue for the organization. According to Chung *"The internet stands as a collection of privately owned servers and end hosts a resource theoretically belonging to everyone. The power to shut it down, many argue, shouldn't exist in the hands of a single person or organization."* Network engineers work closely with these servers and have full control over them. Any approaches taken when it comes to mitigating risks and protecting the assets of the organization must be handled delicately.

Determinism is the principle that examines the minds of criminals and what caused them to commit the crime. The job of a Network Engineer is to protect the organization from vulnerabilities and cyberattacks. Behind these crimes there is always a reason behind why they were committed. It could be for reasons such as financial gain or to even get back at an old manager that they may have felt wronged them during their time with the organization. According to Neufeld*, "Research suggests that many computer-enabled crimes are hidden from view and go unreported due to victim ignorance, fear of consequential impacts (e.g., panic, loss of public confidence, reputational damage), quantification difficulty, and lack of victim motivation (Chan, **2000**), thus it is difficult to pinpoint the precise scope and scale of the computer crime phenomenon." (p. 1.)* I thought that this was an interesting perspective in regard to cybercrime. Determinism suggests that we have free will and that criminals choose to carry out these actions, however in order to minimize these actions from occurring we have to ask questions about what caused them to act on their behavior. An example of this within the network engineering field would be trying to figure out why someone tried to hack into the systems of the organization. Theres are plenty of reasons why this may have occurred, but we won't know until we study and question the individual to gain some insight into the situation.

Regarding marginalized groups, especially within the cybersecurity field, I feel that it is important to conduct social research studies to get a better understanding of how things such as crimes affect those groups. Workers within major organizations and the average citizen who uses the interest to conduct activities online would be part of that group. As mentioned in the article Cyber security: challenges for society- literature review *"Threats to cyber security can be roughly divided into two general categories: actions aimed at and intended to damage or destroy cyber systems (—cyber-attacks‖) and actions that seek to exploit the cyberinfrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure (—cyber exploitation‖) [8]."* These threats can have major impacts on both consumers and workers alike. As a network engineer, it is important to find ways to mitigate these threats to not only minimize them but protect both the organization and individual from having any sensitive information exploited from crime.

Chung, Alex, and Chi Xing. "The Ethics of Net Neutrality." UCDavis Computer Science (2011).

Neufeld, Derrick. "Computer crime motives: Do we have it right?." Sociology Compass 17.4 (2023): e13077.

Tonge, Atul M., Suraj S. Kasture, and Surbhi R. Chaudhari. "Cyber security: challenges for society-literature review." IOSR Journal of computer Engineering 2.12 (2013): 67-75.