Adeline Harris

Reflection Essay

This course and all the work done in it have been very vital in helping me understand how to approach my career goal in cybersecurity. Looking into the ethical tools provided by the course, the first thing I learned was how diversified the study of ethics is. I always had the idea that all ethics was generally classified and understood as the same. Seeing different tools for it, and how they dictated the ethical style being practiced along with its application, was a very good eye-opener. Tools like contractarianism, Ubuntu, virtue ethics, and utilitarianism give a clear understanding of relational ethics and how it works. Learning the value of privacy as it relates to these tools of ethics proved essential in knowing how my role as a security analyst would serve to protect it and why. Every case analysis and the challenges they presented allowed for a look at each tool in practice. Utilitarianism allows us to consider what it would be like if policies are made in consideration of all people, looking to the betterment of all. In similar fashion, contractarianism shows how observing socially agreed-upon morals serves as a guide in organizational alongside societal dynamics. Understanding these dynamics put the concept of virtue ethics into perspective, which is reinforced by the case analyses. Acting virtuously is only valuable based on the scenario and how the action taken benefits society. Virtue ethics shows that, if done for a virtuous reason, even whistleblowing in an almost disloyal way can be ethical. Then there is my personal favorite, Ubuntu, which talks of community and how a person is a person through persons. All these tools coming together are shaping my ethical view as a cybersecurity analyst. It

makes it clear that in all my work, as in my study, the primary goal should be for the good of all people and society.

Another important thing this course changed for me was my understanding of cyberwarfare and information warfare. Before this class, I mostly understood cybersecurity from a technical perspective involving systems, networks, malware, and protection against attacks. While those things are still important, this course made me realize that cybersecurity also has a very human and political side to it. Looking at cases involving cyberconflict, whistleblowing, surveillance, and information warfare showed me that technology is never really separate from society. It is always connected to people, governments, beliefs, and power. This added much more nuance to how I understand cybersecurity and the responsibilities that come with it.

The discussions on information warfare especially deepened my understanding of how dangerous the manipulation of information can be. I had always thought of warfare mostly in the physical sense, but this course showed that warfare can also happen psychologically through cyberspace and social media. Looking at how nations and organizations use misinformation, propaganda, bots, and trends to influence public opinion made me realize how powerful information itself can become. The idea that people can be manipulated emotionally through algorithms and carefully spread narratives was something I had not fully considered before. Through the case analyses and readings from authors like Morkevicius and Jarred Prier, I came to understand that cyberspace has become another battlefield where influence and perception are constantly being contested.

The whistleblowing cases also gave me a different perspective on privacy, loyalty, and morality. Before this course, I mostly viewed whistleblowing as simply exposing secrets, but now I see that it can be much more ethically complicated than that. Cases involving people

like Chelsea Manning and Edward Snowden showed that there are situations where exposing information may be done because someone believes the public deserves to know the truth. Even though these actions may break laws or organizational loyalty, ethical tools like virtue ethics and Ubuntu make it possible to evaluate the intention and effect behind those actions differently. This gave me a more balanced perspective because I now understand that ethical decisions in cybersecurity are rarely completely black and white.

A major takeaway from this course for my future career is that cybersecurity is not only about protecting systems, but also about protecting people, trust, privacy, and community. The ethical tools learned throughout the semester have helped shape how I want to approach situations in the future. Whether dealing with user privacy, organizational policy, cyberwarfare, or digital misinformation, I now understand that the decisions made in cybersecurity can affect entire communities and societies. Because of this, I believe that technical skill alone is not enough. A cybersecurity professional must also have ethical understanding and good judgment. This course has therefore helped me develop not only academically, but also personally, by changing the way I think about technology, responsibility, and the impact cybersecurity has on society as a whole.