

Reflection on Cybersecurity Ethics: Evolving Perspectives and Enduring Lessons

Over the course of PHIL 355E: Cybersecurity Ethics, I've had the opportunity to examine how ethical frameworks apply to digital systems, cybersecurity professionals, and corporate structures. Three key areas that particularly shaped my thinking were corporate social responsibility (CSR) in the tech sector, the professional ethics of cybersecurity practitioners, and the ethical dimensions of cyberconflict. My understanding of each topic has deepened not necessarily by flipping my initial positions, but by adding nuance, recognizing competing values, and thinking more critically about the ethical weight of decisions in digital spaces.

Corporate Social Responsibility in Cybersecurity

When I first observed corporate social responsibility (CSR), I saw it primarily as a public relations strategy, something large companies used to bolster their image rather than to enact genuine change. In the context of cybersecurity, this often appeared as vague statements about “protecting users” or “being transparent,” without much accountability or ethical depth.

However, as we explored more about the structural and moral obligations of corporations, especially through the lens of philosophers like Milton Friedman, who argue that the sole social responsibility of business is to increase its profits, within the boundaries of the law. I began to see CSR not as a façade, but as a necessary ethical framework for evaluating corporate action in digital spaces.

What shifted most for me was understanding the depth of responsibility tech companies carry. It's not just about avoiding harm but actively promoting digital justice. For instance, companies that manage sensitive data (like social media platforms or cloud providers) aren't just

stewards of code, they are powerful actors shaping human rights, privacy, and democracy. When we discussed cases involving emphasizes that companies should actively participate in defining a new social contract that incorporates ethical considerations, environmental stewardship, and community engagement. It became clear to me that CSR in cybersecurity must be more than an afterthought but a design principle.

Professional Ethics and the Role of the Cybersecurity Expert

Coming into the course, I thought of cybersecurity professionals as mostly technical problem-solvers people responsible for patching vulnerabilities, stopping hacks, and building secure systems. I hadn't given much thought to their ethical obligations beyond general integrity. But after studying frameworks like the ACM Code of Ethics and examining real-life whistleblower cases (like Edward Snowden or the more recent Frances Haugen), I began to appreciate the unique ethical challenges cybersecurity professionals face.

They often operate in high-stakes environments where the consequences of their work aren't just technical, they are political, personal, and even existential. We read about situations where professionals had to choose between loyalty to an employer and their broader responsibility to society. This really made me reflect on the difference between being a "good employee" and a "good professional." The former follows orders; the latter follow ethical principles, even when they conflict with organizational goals.

As a future professional, I want to be guided by ethical courage: the willingness to speak up or act when something is wrong, even when it's inconvenient, risky, or unpopular.

Cyberconflict and the Ethics of Digital War

Cyberconflict was probably the most complex and unfamiliar topic for me. Initially, I viewed cyberwarfare as a modern extension of espionage something governments did to each other, far removed from ordinary life. But the more we studied the ethics of cyberattacks, critical infrastructure vulnerabilities, and the blurred lines between civilian and combatant, the more unsettled I became.

We explored traditional just war theory, *jus ad bellum* and *jus in bello* and how these concepts struggle to apply in digital contexts. For example, how do we define a "proportional" response to a ransomware attack that disrupts a hospital network? Who should be held responsible when attribution is murky or obscured? These aren't just philosophical questions, they affect how nations respond, how civilians are protected, and how escalation is managed in an already fragile geopolitical environment.

The topic pushed me to reconsider how digital tools amplify the moral risks of war. The asymmetrical cyberconflict where small groups or even individuals can cause enormous harm makes it even more important that we develop strong ethical and legal frameworks before these conflicts escalate beyond control.

The rules of engagement in cyberspace are still being written. I want to stay informed and advocate for ethical norms that prioritize civilian safety, transparency, and restraint in digital conflict.

Final Thoughts

This course has challenged me to think more rigorously and responsibly about how power, knowledge, and ethics intersect in the digital world. These three topics CSR, professional

ethics, and cyberconflict aren't just academic; they are deeply relevant to the kind of professional I want to be and the kind of world I want to help shape. As technology continues to evolve, I hope my ethical reasoning evolves with it, guided not just by technical skill but by thoughtful, principled reflection.