

Kunal Patel

12/10/2024

PHIL 355E: Cybersecurity Ethics

Dr. Alice Q. Fox

Old Dominion University

Reflective Writing Assignment

This semester has been transformative in deepening my understanding of cybersecurity's ethical, theoretical, and practical dimensions. Throughout this reflection on materials, I have identified three key topics important in shaping my thinking: Professional Ethics in Software Development, whistleblowing ethics, and ethics of cyberconflict. Accordingly, each subject area has provided essential lessons regarding my future cybersecurity profession or broader ethical considerations.

1. Professional Ethics in Software Development: Responsibility and Integrity

The case of Bill Sourour's pharmaceutical quiz, which directed users to a particular drug despite known risks, accentuated the importance of professional ethics in software development. Initially, I perceived software development as a purely technical discipline. However, the story of Sourour enlightened me on how great an ethical responsibility developers carry in protecting public trust and preventing harm.

In other words, through deontological ethics and the ACM Code of Ethics, I learned that developers must be forthright, prevent harm, and be responsible. Because Sourour failed to design an honest tool that protected users from damage, it underlined how much moral courage was needed to attend to an unethical directive. The professionals have to be on the side of transparency and consider user safety, even if at the personal or professional risk of loss.

Takeaway: I will maintain integrity and accountability in my career and ensure my work demonstrates ethical principles. I will contribute to system development based on professional codes that are in the best interest of honesty and safety for the general public.

2. Whistleblowing Ethics: Moral Courage and Loyalty

Whistleblowing through Chelsea Manning's actions made me examine loyalty and ethical responsibility more closely. Initially, I considered whistleblowing to be an act of betrayal; however, the frameworks of Vandekerckhove and Oxley & Wittkower unraveled it as higher moral loyalty to justice and public accountability.

Manning's decision to leak the "Collateral Murder" video exposing human rights violations is a perfect example of ethical responsibility regarding whistleblowing. This case underlines a fundamental concept called conditional loyalty- the loyalty one owes to an organization whenever it acts ethically. Manning showed moral courage by placing human dignity over and above institutional loyalty, which has rewritten my perception of professional ethics.

Takeaway: I will exercise ethical integrity and be constantly watchful for institutionalized wrongdoing. As a cybersecurity professional, I must balance my loyalty to my organization against the commitment to justice and accountability by ensuring my actions are in the best interest of higher ethical values.

3. Ethics of Cyberconflict: Just War Principles and Accountability

Cyberconflict, particularly the ethical dilemmas surrounding attacks on civilian infrastructure, challenged my assumptions about the morality of digital warfare. While I initially viewed cyberwarfare as less hurtful than traditional conflicts, analyses regarding the Russia-Ukraine conflict and the Stuxnet attack emphasized the severe ethical challenges posed by cyberattacks.

Boylan's principles of discrimination and proportionality stress the requirement to minimize civilian harm, while Taddeo's framework emphasizes accountability within cyber operations. Most cyberattacks against such facilities as power plants or hospitals blur the line between combatants and non-combatants, causing disproportionate damage. These cases underlined the ethical hazards of cyberwarfare and the imperative for accountability and restraint in using cyber capabilities.

Takeaway: Ethical principles must guide the development and deployment of cyber tools. As a cybersecurity professional, I will support a policy prioritizing civilian protection by the just war theory, serving humanity without compromising key rights.

Conclusion

This semester's exposure to professional ethics, whistleblowing, and cyberconflict has shaped my ethical framework and professional aspirations. Each of these topics underlined the importance of keeping human rights, accountability, and justice at the core of all efforts within cybersecurity. These lessons will act as an enduring compass for me as I journey into this field, reminding me of the high level of ethics one needs to maintain when there are difficult situations to address. I seek to contribute to a more secure and equitable digital world by integrating these principles into my practice.