Liam Redman 01214332

May 1, 2024

PHIL 355E

Professor Nicol

During my time in this course, I have explored many complex and multifaceted topics in cybersecurity. These case studies have significantly enriched my understanding and perspective on key issues affecting both global politics and individual freedoms. In this paper I will reflect on the three topics that I was most interested in; Information Warfare, Cyber Conflict, and Whistleblowing, discussing how my views have evolved and showcasing the key takeaways I have taken from this course

`At the beginning of this course, my view on Facebook's involvement in information warfare was somewhat simplistic, viewing it primarily as a platform misused by malicious actors. However, as I delved deeper into the mechanics of how Facebook's algorithms and business model may inadvertently lead to such misuse, my perspective shifted. I now see Facebook not just as a passive tool, but as an active participant with significant responsibility in the propagation of disinformation. Through case studies, particularly examining the 2016 U.S. Presidential Election, I recognized that Facebook's algorithmic decisions are designed to maximize user engagement and also maximize the spread of misinformation. This has led me to appreciate the complex interplay between technology design and the ethical responsibilities of tech companies. The discussions and readings highlighted the real-world consequences of technological neutrality, where even a platform's non-decision becomes a decision with immense

impact. My key takeaway was to always consider the broader ethical implications of technology design and business models. As a hopeful future professional in the tech field, I must advocate for and implement responsible technologies that consider potential misuses and mitigate harm to democratic processes.

Discussing the ongoing cyberconflict between Israel and Iran, where both nations engage in cyberattacks against each other's infrastructure, challenged my initial black-and-white views on justice and national security. Initially, I believed that such acts were straightforwardly unjust, categorizing all forms of offensive cyber operations as negative. However, studying the complexities of international relations and national defense, I have come to understand these cyber operations within the broader context of deterrence and defense. This perspective recognizes that while cyberconflict can escalate tensions and lead to significant consequences, it also serves as a tool for states to assert power and protect national interests without resorting to conventional warfare, which would have far more devastating physical effects. My key takeaway In the realm of international cybersecurity is that ethical judgments must be contextual. Actions considered 'unjust' in isolation may be part of broader defensive strategies. It's crucial to balance ethical considerations with practical realities in international relations.

At first, I viewed Chelsea Manning's disclosure of classified information purely as a courageous act of whistleblowing that exposed government wrongdoings. However, through class discussions and readings, I gained a deeper understanding of the ethical, legal, and personal complexities involved in whistleblowing. The view I now hold recognizes both the ethical justification for Manning's actions in exposing human rights abuses and the potential risks and unintended consequences of such disclosures. This nuanced understanding has taught me that

whistleblowing is a multifaceted issue where the ethical justification heavily depends on the whistleblower's intentions, the sensitivity of the disclosed information, and the potential impact on public interest and national security. My key takeaway is that Ethical whistleblowing should balance the public's right to know against potential harms. Future actions in similar situations should strive for responsible disclosure, where possible, to minimize harm while maximizing the benefit to society.