Liam Redman 01214332

April 15th, 2024

PHIL 355E

Professor Nicol

The ongoing cyberwar between Israel and Iran, represents a growing deep rooted problem, manifesting through sophisticated digital skirmishes that affect vital national infrastructures and civilian life. Historically, these attacks have not only targeted military or governmental assets but have also jeopardized public utilities and economic structures, intensifying the stakes of their long-standing regional rivalry. Notable incidents include Iran's alleged disruptions of Israeli water supply systems, which threatened public health, and Israel's purported cyberattacks that disabled Iranian port operations, causing significant logistical and economic disruptions. These cyberattacks blur the lines between military and civilian targets, leading to a scenario where the unintended consequences on ordinary citizens are significant and morally problematic. In this case analysis, I will argue that Deontology, particularly through a Kantian lens, demonstrates that the cyberwar between Israel and Iran is not just because it systematically fails to respect the intrinsic moral rights of individuals affected by these attacks

Michael Boylan's work "Can There Be a Just Cyber War?" delves into the ethical underpinnings of cyber warfare, extending the traditional just war theory into the digital realm. This theory traditionally includes principles like jus ad bellum (the right to go to war) and jus in bello (the right conduct in war), which Boylan adapts to address the unique challenges posed by cyber conflicts. These adaptations are crucial for evaluating the ethical dimensions of initiating and conducting cyber warfare.

In applying Boylan's adapted just war concepts to the cyberwar between Israel and Iran, it's essential to examine the motivations and conduct of both nations. The jus ad bellum criteria require a just cause, typically self-defense or the prevention of imminent harm. Israel and Iran have both justified their cyber operations under the guise of self-defense. Iran might claim its cyberattacks on Israeli infrastructure, such as the water supply system, are preemptive strikes to discourage Israeli aggressions, including alleged cyber intrusions into its nuclear facilities. Conversely, Israel might argue its cyber strikes on Iranian ports are necessary to deter or delay Iran's potential nuclear weapons development.Yet, according to Boylan's interpretation, these justifications must be scrutinized against just war criteria like proportionality and necessity. The principle of proportionality demands that the damage inflicted by military operations should not exceed what is necessary to achieve legitimate military objectives. The targeting of civilian infrastructure like water systems raises ethical concerns, as it can lead to significant civilian suffering, which may outweigh the military advantages gained. Similarly, the necessity criterion questions whether these cyber operations were the last resort after all other non-military options had been exhausted.

From a deontological standpoint, which emphasizes the morality of actions themselves rather than the outcomes they produce, the ethical analysis shifts focus. Deontology, particularly Kantian ethics, argues that actions must respect the dignity and rights of all individuals, treating them as ends in themselves and not merely as means to an end. Applying this to cyberwar, any action that treats civilians and their essential services as tools for achieving military or political objectives—such as disrupting a nation's water supply or crippling port operations—fails to meet these ethical standards. Both Israel and Iran's cyber strategies, when they impact civilian life and infrastructure, seem to disregard these principles. Such actions can be viewed as using individuals as pawns in a broader geopolitical game, which Kantian ethics explicitly condemns. The deontological perspective would criticize both nations for not adhering to ethical conduct that respects the autonomy and inherent worth of every individual affected by their actions.

Based on the deontological analysis, the right thing to have done for both Israel and Iran would have been to strictly limit their cyber operations to legitimate military targets and avoid any actions that could foreseeably lead to civilian harm. This would involve rigorous ethical oversight and possibly the development of international norms and agreements that clearly define acceptable targets and tactics in cyber warfare. The aim would be to ensure that all actions adhere to a universal moral law that upholds the dignity and rights of individuals, aligning with the Kantian imperative to treat humanity always as an end in itself, never as a means to an end. Thus, a just cyberwar, if it is possible at all, would require adherence to both traditional just war principles and strict deontological ethics, ensuring that all actions are justified not only by their causes but also by their respect for human rights and dignity.

Mariarosaria Taddeo’s work, "An Analysis for a Just Cyber Warfare," presented at the 4th International Conference on Cyber Conflict, explores the ethical dimensions of cyber warfare. One of her central concerns is the difficulty of ensuring discrimination and proportionality in cyber operations—key ethical criteria in traditional warfare, which become blurred in the cyber context. Discrimination here refers to the ability to distinguish between military and civilian targets in an attack, while proportionality assesses whether the scale of an attack is appropriate to its military necessity and avoids excessive harm.

In the ongoing cyber conflict between Israel and Iran, both countries have reportedly targeted infrastructure that, while possibly connected to their respective nation's security concerns, also impacts civilian populations. For instance, cyberattacks on power grids or water treatment facilities disrupt services essential to civilian life and may not strictly qualify as military targets. These actions highlight the challenge of discrimination in cyber warfare, as the attacks affect both civilian and potential military components of the target nation.Furthermore, the issue of proportionality is equally problematic. Cyberattacks that lead to widespread disruption of civilian life can be seen as disproportionate if the original military objective does not justify such extensive collateral damage. For example, disabling a national power grid to impair military communications could also endanger hospitals, emergency services, and basic civil operations, leading to outcomes that far exceed the intended military benefits.

From a deontological perspective, the moral evaluation of these cyber operations hinges on the principle of treating individuals as ends in themselves and not merely as means to an end. Kantian ethics insists on the inherent dignity of all persons, requiring that actions respect and preserve this dignity.When applied to the cyber conflict between Israel and Iran, many of the cyber operations appear problematic. If cyberattacks indiscriminately affect civilian populations, they violate the Kantian imperative by treating these civilians as mere tools in achieving strategic objectives. For instance, attacking civilian infrastructure to pressure a government or disrupt an economy treats those affected civilians not as individuals with rights and dignity but as instruments of warfare.This perspective starkly contrasts with a deontological ethical approach, which would mandate actions that respect the moral rights of all individuals involved, ensuring that any military action strictly targets combatants and military assets, avoiding harm to civilians wherever possible.

Based on Taddeo's analysis integrated with deontological ethics, a more ethical approach to cyber warfare between Israel and Iran would involve a stringent application of discrimination and proportionality principles. Both nations should strive to develop and adhere to clear guidelines that ensure cyber operations are targeted, limited, and justifiable under these ethical standards. This includes avoiding any targets where civilian harm is foreseeable and disproportionate to the military gains. Moreover, international cooperation and dialogue might be necessary to establish and enforce norms that govern cyber warfare, creating accountability mechanisms that help ensure actions remain within ethical bounds. By committing to these principles, Israel and Iran can help ensure that their cyber warfare tactics not only serve their security interests but also respect the fundamental ethical requirement of protecting civilian lives and dignity.

In examining the ethical dynamics of the Israel-Iran cyber conflict through the perspectives of Michael Boylan, Mariarosaria Taddeo, and Kantian ethics, it's clear that ethical conduct in cyber warfare is complex and challenging. These frameworks highlight the necessity for justified, discriminating actions in cyber operations. This tension between ideal ethical standards and the practical demands of cybersecurity highlights the need for adaptable ethical applications. Ethical theories provide essential guidelines, but their application must accommodate the uncertainties of modern cyber warfare. A balanced approach is therefore crucial, aiming to maintain ethical standards while recognizing practical limitations and strategic necessities. This pragmatic yet principled strategy is essential for navigating the ethical dilemmas in today's cyber conflicts, ensuring that actions are both effective and ethically sound. One key objection to this approach could be its practicality. In real-world scenarios, the rapid pace and ambiguous nature of cyber threats might compel nations to act in ways that stretch or even bypass these ethical boundaries to protect national security or prevent greater harms. This highlights a significant tension between ideal ethical standards and the practical demands of national defense in the cyber domain.