Ava Baratz

CYSE 355

Professor Montoya

November 14, 2022

Cyber Warfare

As the world technologically advances, countries have sought out cyber warfare as a modern approach to physical combat. Cyber warfare is not inherently destructive, however, possibilities to cause immense destruction to arise depending on how cyber attacks are implemented. Iran and Israel have been engaging in cyberattacks for over ten years with recent years bringing significant, harmful implications to citizens present in each country. In *The Cyberwar Between Israel And Iran Is Heating Up",* Dr. Adnan Amer explains how the cyberwar has progressed into a harmful battle with increasing tensions, placing citizens' lives on both sides in jeopardy. Both sides commence attacks that target primarily the infrastructure of the opposing country which affects the safety of individuals. For example, Iran targeted one of Israel's largest hospitals, forcing doctors to engage in manual procedures. The complete system server shutdown at this hospital placed many innocent lives at risk. In addition, Iran targeted Israeli water systems, leaving Israeli citizens' safety at risk by eliminating clean drinking water. Israel's president expressed concerns about Israel's lack of preparedness with many anticipating a decline in the general economy, potentially leading to an impact on the Israeli quality of life.

Likewise, Israel has been targeting Iran's infrastructure in response to anticipated attacks. Israel targeted a major Iranian railway recently, preventing thousands of trips. In addition, Israel attacked Iranian gas stations, disabling Iranian citizens from engaging in daily obligations. The effect of shutting down gas stations caused chaos for Iranian citizens. In this case analysis, I will argue that deontology shows us that the cyber war between Israel and Iran is not just because it treats others unfairly by imposing safety risks on innocent citizens and creating opportunities for mass destruction on each side.

Can There Be A Just Cyber War? Micheal Boylan explains that in Just War Theory, which determines the morality guidelines to engage in war, establishes target distinction. In standard, physical combat, a war can be considered moral if it exclusively targets opponents and avoids harm to innocent non-combat citizens. Military forces are obligated to engage in attacks on the battlefield to avoid collective harm to the general while accomplishing military goals. Cyber warfare, however, primarily consists of attacks targeted around civil infrastructure that affect the whole of society. Due to its nature, it affects combat individuals and innocent citizens. Cyber warfare almost eliminates the possibility to ensure target distinction. Boylan further demonstrates his argument by highlighting the possible harmful effects of cyber warfare on citizens. Boylan discusses the possibilities for death that arise as public infrastructure is targeted. For example, if a group of people targets air traffic control and intentionally causes a plane to malfunction, many innocent lives are placed at risk. Similarly, public safety can become compromised if hackers cause electricity shortages within a city. Those residing at a hospital become at risk of passing away as doctors no longer have sufficient methods to treat their patients.

Lack of target distinction is ubiquitous throughout the cyber war between Iran and Israel as innocent citizens fall victim to warfare. The technology used in these attacks is unable to distinguish between combat forces and civilians. In return, all individuals present in Iran and

Israel are targeted and forced to endure the severe ramifications of war. Although some may argue this cyberwarfare is just because it does not intentionally kill others, the destruction and way it is implemented create significant harm to society in both countries. There is no target distinction present as individuals in both countries suffer the impact of having compromised infrastructure. For example, with the Israeli attack on Iranian gasoline, they were unable to specifically direct their attack to one group of people. Because of this, the entirety of Iran suffered the consequences of being unable to obtain gasoline. Likewise, when Iran targeted Israeli water systems, they were unable to target a particular group of individuals. Instead, the entirety of Iran obtained contaminated water, placing many lives at risk.

While considering the actions of the cyber war through a Deontological approach, it is evident that this war is unjust. Deontology prioritizes behavioral obligations to act morally all the time, disregarding any exceptions. Deontology demands absolute respect for others in addition to being fair to others. The effects of the cyber war disregard deontology completely, as citizens are placed at an unfair advantage of risk safety. However, both countries can use Deontology in cyber warfare to ensure all citizens are respected and are allowed consent for actions taken in war. Countries can take this approach to eliminate attacks on public infrastructure that targets every individual. Instead, countries can mandate attacks that exclusively affect the persons of interest in the opposing country. For example, Iran may only target a weapon factory in Israel. This way, no individual’s safety is compromised and only the specific target is attacked. Countries should establish open communication regarding specific acts of war with their citizens to allow citizens to consent to the country’s actions and whether they would be affected in any manner.

In *An Analysis Of Just Cyberwarfare* by Professor Mariarosariah Toddeo, Toddeo explains how cyberwarfare is not “necessarily” violent when compared to traditional war combat. Taddeo describes how cyberwarfare can become destructive as non-combative citizens are targeted. Engaging in cyberwarfare that exclusively targets informational infrastructure, such as databases, results in less destruction and fewer casualties. Taddeo argues that to engage in cyber warfare, a country must adhere to ethical guidelines to ensure fairness. In addition, countries are encouraged to use war as a last resort. Considering cyber warfare through the principle of information ethics allows countries to assess the morality of actions as information objects with individual rights. This theory examines a given action’s effects on others and the infosphere in which all communications and data are received and stored. Taddeo states that countries should only engage in cyber warfare if it increases the overall good and further eliminates evil within the infosphere. Countries must prioritize the state of the infosphere before and after cyber warfare. Taddeo further describes how anything that produces immoral outcomes loses rights in the infosphere as it interferes with the well-being of others.

After examining the informational ethics approach to cyber warfare, it is evident that the actions taken are not just by increasing the amount of evil in the infosphere. When scrutinized closely, Israel and Iran’s acts of war are not beneficial. These acts contribute to polluting the infosphere with evil as malicious attacks are initiated. Each country is engaging in cyber warfare in a way that goes back and forth, with increasing intensity each time. These countries are not engaging in attacks that better the overall utility of the infosphere and society. Instead, these countries contribute to the suffering of the infosphere as there is mass destruction created for insignificant reasons. For example, data in hospitals are compromised with minimal valid motives. Overall, these actions leave their citizen’s safety at risk and threaten the economy of both countries. Both countries disregard the morality of their actions and instead, attack in hopes of producing a more increasingly impactful attack on their opponent.

Through the use of Deontology, both countries can consider their actions more carefully while placing value on consistently acting morally, ensuring a just war. This way, both countries can think through all possible implications of an action before it is commenced. This way, countries can consider bettering the overall infosphere and create less harm for their citizens. This way, their citizens are being considered in a way that provides absolute respect. For example, before either country attacks an infrastructure that may harm a country's citizens, the country needs to contemplate the attack's benefit regarding the infosphere. If it is not contributing to the infosphere's utility, then the country must move forward with the attack. This careful consideration shows that a country contributes effort towards acting morally. Either country must not make any exception for themselves as they consider each action possible. This way, the countries are held accountable for their actions and consider morality as the determining factor in progressing with their actions.

Although the ongoing cyber warfare between Israel and Iran does not intentionally attack individuals, deontology illustrates the war as unjust as many lives are at risk in both countries. This cyber warfare repeatedly attacks public infrastructure that disrupts the safety of individuals present in both countries. Cyber warfare does not allow for target distinction to ensure the attacks exclusively affect those intended. Instead, everyone suffers the ramifications of cyber warfare. In addition, the acts in the cyberwar between Israel and Iran do not benefit the overall utility of society and its infosphere. These countries do not assess their actions considering morality. Rather, their actions present an apparent lack of respect for their citizens and do not allow for free consent regarding specific war actions. This cyberwar can serve as an example of unjust attacks for future conflicts. As society keeps technologically progressing, it is imperative to act ethically during engagement in cyberwarfare as it can easily cause worldwide destruction if handled inappropriately.