For over the past two decades, Iran and Isreal have been engaged in a cyber war. This has included attacks on integral systems such as fuel, electricity, and healthcare. For example, in 2021 Iran experienced a loss in the ability to dispense fuel to Iranians due a cyberattack on its systems. While no particular country or group claimed responsibility and Iran's leader did not blame any specific country, given the history of each country using cyber means to attack the other and not officially releasing a statement about it, along with comments from Iran suggesting it was "anti-Iranian" forces that may be responsible, Isreal appears as a likely option.

This particular war is significantly different from other conflicts due to the fact that attacks are being done through the cyber world rather than through ground troop deployment and operations. This complicates evaluating whether this cyberwar is ethically just or not. Do the same principles and theories used to justify traditional wars hold the same weight in this particular conflict? In this Case Analysis I will argue that consequentialism shows us that the cyberwar between Isreal and Iran, as a whole, is not ethically just due the war's high risk for negative or unpredictable outcomes such as civilian harm.

Michael Boylan considers if, (and if so, how) the Just War theory applies to the concept of cyberwarfare in his paper "*Can There Be a Just Cyber War?*". First, he makes the distinction that an instance of sabotage and an instance of cyberwarfare are two separate concepts whose distinction depends on the degree of severity. He gives the example that if there is an instance of sabotage that shuts down a company for a short period of time and is used to steal information, that is a more minor degree of severity compared to an instance of cyberwarfare that disables a country's military systems.

Additionally, he brings up two concepts from the Just War theory: *jus ad bellum* and *jus in bello*. *Jus ad bellum* , or "right to go to war" are principles that govern when it is permissible to go to war, and *just in bello* , or “right conduct in war”, focuses on the rules concerning conduct during warfare. Both of these concepts are utilized within the Just War theory in order to evaluate the ethical reasoning behind warfare as a whole. However, Boylan brings up that the nature of cyberwarfare differs from the traditional means that were used to form the Just War theory, and that changes should be considered to better fit the current climate of global conflict.

His reasoning for suggesting changes be made is due to a number of factors. Firstly, as opposed to the traditional paradigm of the Just War theory, in cyberwarfare, killing is not always primary. Additionally, it is not always clear who committed the act of war, as territoriality and neutrality are blurred. Just because two countries have physical distance between them does not mean that a cyber attack cannot reach the other. Delivery of the attack is done via the Internet or other means, such as a flash drive. When applying Boylan’s points of how the traditional meanings behind the Just War theory differs from the concept of cyberwar to the case of Isreal and Iran, it is clear to see that this theory is currently not in a state in which it can be used as justification for the war itself.

A key concept of a consequentialist outlook is to focus on the outcomes of an action and use these outcomes to determine if an act or decision was ethical. Concerning the cyberwar currently going on between Isreal and Iran, the outcomes could result in extremely negative consequences, namely human injuries or casualties. While cyberwarfare tends to avoid direct human harm, specifically when compared to traditional warfare means, it does not mean that this form of warfare can not cause *indirect* harm. Take a case concerning an attack on a hospital’s online systems for example. The attack itself only focuses on the systems themselves; no human harm is directly caused. The outcomes, however, have a high potential to result in harm to human lives. Without sufficient access to important systems, these hospitals will not be able to give efficient care to their patients. Whether this was an intended outcome or not, the negative outcome, when considered using a consequentialist view, identifies this attack as unethical.

Mariarosaria Taddeo also discusses the Just War theory and how it applies to cyberwarfare in her paper "*An Analysis for a Just Cyber Warfare*". However, she points out that while considering the Just War theory when considering cyberwarfare is necessary, it is not sufficient to fully address all of the nuances and complexities that cyberwarfare presents. She also states that while cyberwarfare appears to not necessarily a violent phenomenon that does not involve human beings, humans still are required to be involved as these attacks need to be designed and effectively implemented. Taddeo also presents three issues with how the Just War theory addresses warfare that would prevent it from efficiently evaluating cyberwarfare: 'war as a last resort', 'more good than harm', and of 'non-combatant immunity'.

'War as a last resort' dictates that a state may only resort to war in the case of having exhausted all reasonable alternatives to the conflict in question. This principle assumes that the war is always violent, which as Taddeo has established, is not always directly violent in nature. 'More good than harm' relates to the idea that before declaring war, a state must consider what global good that is expected to follow the conflicts against the negatives. On a surface, direct level, cyberwarfare automatically fits this principle as it is not necessarily directly violent. Finally, the 'principle of discrimination and non-combatant immunity' concerns the distinction between those involved in combat and uninvolved citizens. In the case of cyberwarfare, this distinction can be muddied as operations can be done outside of governmental complexes or other expected areas. Taddeo goes further to point out that if combatants can easily hide themselves among the civilian population, the state may be justified in endorsing high levels of surveillance over the entire population, introducing the potential breach of individual rights surrounding privacy.

One of these principles bears similarities to the principles of consequentialism: ‘more good than harm’. Taddeo points out that on the surface, the concept of cyber war often always fits this principle since there is no violence or direct harm. I would agree with the point that it does not *directly* cause harm to a state’s civilian population and infrastructure. However, there are opportunities for harm to be caused as a result of a cyberwarfare attack. For example, like I discussed earlier, interruption to critical infrastructure can directly cause human casualty. Additionally, cyberwarfare being utilized and subsequentially normalized poses a risk that these kinds of attacks which are pointed towards systems that could have negative outcomes for the civilian population could see an increase in usage. A theoretical increase in cyber-attacks in a warfare setting has the opportunity to be just as destructive to both combatants and civilians, if not more destructive, than traditional land-based warfare.

The continuous cyber war that has been occurring between Isreal and Iran for the past few decades has exemplified a shift in the way that the term “warfare” is considered. The term that once described global conflict that occurs on land, sea, or air using ground troops has begun to change into a kind of conflict that occurs more indirectly using strategic cyber means, negating the need for close geophysical distance. This shift in understanding raises questions about how efficient the current theories and principles that are currently established for determine the ethical justifications of war are. When evaluating this particular case between Isreal and Iran, consequentialism can be used to determine that this case of cyberwarfare is not just. Consequentialism evaluates the ethical nature of an action based on what outcomes have already, or have the potential to, occur. A direct opposing ethical philosophy in this case to consequentialism is deontology, which examines the intent behind the action to determine its ethical status. In a deontological view, the potential and intent for safety and protection behind some of the actions concerning cyberwarfare justifies any negative outcomes. I feel, however, that the weight of the negative outcomes and their potential severity call for a more consequentialist view in this case.