Atticus Emilsson

PHIL 355E

Module 6

6.4 Case Analysis on Cyberconflict

The tensions between Iran and Israel grow ever more as made apparent by the articles. In the articles presented by Dr Adnan Abu Amer and Chantal Da Silva, the increasing fears amongst civilians in these countries rise. The uncertainty proposed by the transversality of cyber conflict continues to grow, and each country continues taking retaliatory strikes at one another. These attacks present themselves to simply assert power rather than to reach an accord. The threats posed to civilian/non-combatant lives rise as the intensity of the cyber-attacks increases. This threatens our current understanding and implementation of JWT (Just War Theory), calling for a revisit of what constitutes a just war. In this Case Analysis I will argue that Kantianism shows us that the cyberwar between Israel and Iran is not justified because of an egregious ignorance of the principles set forth by the JWT, which emphasizes the importance of the preservation of civilian/non-combatant lives.

In the article titled *Can there be a Just Cyber War* by Professor Michael Boylan, he recognizes the importance of JWT and its shortcomings when applied to Cyberwarfare compared to traditional warfare. In his attempts to address the shortcomings of JWT in its application to Cyberwarfare, he emphasizes integrating any newfound ideas within the preexisting JWT rather than completely reinventing the wheel. He says that he does not suggest we “jettison” JWT, but

rather that it must be “expanded to include the new dynamics of warfare.” These “new dynamics,” of course refer to Cyberwarfare (CW). He, however, recognizes the difficulties that arise when trying to effectively integrate the integral concepts of Cyberwarfare into the predefined JWT. One of the primary difficulties necessitated by JWT is attribution. The ability to attribute an action/result to a certain individual/group is of paramount importance when determining whether an act of war is justified. Failure to properly attribute a group for their actions can also render a body unable to determine intent. These inabilities also inhibit one’s ability to retaliate in a manner that is accurate (aimed at the group attributed to the first strike) and proportional to their infrastructure and their initial strike. Unfortunately, cyberwarfare greatly blurs these lines and makes it incredibly difficult to accurately attribute responsibility for an action to a certain group. It is also incredibly difficult to properly discriminate between combatants and non-combatants (civilians). We can observe this lack of control in a previous act of Cyberwarfare. Stuxnet was an act of Cyberwarfare coordinated by Israel and the United States, which was designed to sabotage an Iranian uranium enrichment facility. Although this Cyberweapon was intended to only affect devices relating to the Iranian facility, it quickly spread out of control and reached the public. This shows that even a long-term collaboration between two world powers is incapable of creating a weapon of Cyberwarfare capable of the necessary degree of discrimination.

In the case of the Cyberconflict that exists between Israel and Iran, each retaliatory strike targets some infrastructure that is critical to civilian living in some manner. This includes the Stuxnet attack, which targeted the centrifuges in the “underground Natanz nuclear facility.” Under the premise that the nuclear program was intended for civilian uses (such as nuclear

power) as they claimed (albeit unlikely), then this could also be considered an attack that targeted infrastructure that would be critical to civilian living. In many of the attacks that allegedly result from either Iran or Israel, there is a certain degree of uncertainty when attempting to attribute the attacks. This failure to accurately attribute these attacks to one another could lead to continued retaliation against civilian infrastructure, and such targeting would be unjust and would be in violation of the currently existing implementation of a JWT.

The intentions exhibited by the warfare between Iran and Israel are not motivated by a desire to reach an accord, to better the welfare of their citizens or society, or to reach a diplomatic solution, but reside simply to assert power. They have consistently failed to properly attribute actions to offending parties and have failed to properly discriminate in their attacks. These continued violations of human rights and the JWT are an egregious violation of ideals presented in Kantianism. Through the lens of the deontological positioning, the actions of warfare between Iran and Israel are not just.

The article titled *An analysis for a just cyber-warfare* by Professor Mariarosaria Taddeo aims to address the shortcomings present in the current implementation of a JWT (which she describes as “necessary but not sufficient”). She also regards JWT and its implementation as important, and crucial to the development and integration of Cyberwarfare and other forms of non-traditional warfare into a JWT. Taddeo’s revision recognizes the complex issue of Cyberwarfare’s inherently transversal nature. In response, she applies a framework of Information Ethics which defines the concept of an Infosphere which is an “environment in which ... informational objects may be morally evaluated” as it relates to JWT and Cyberwarfare.

In the Infosphere, Taddeo prescribes these “informational objects” with the right to “exist and flourish.” Taddeo’s approach which leverages Information Ethics, proposes four “moral principles” which revolve around the concept of “entropy” which she prescribes as an “evil” in a metaphysical manner. This definition of entropy and the four moral principles enable the creation of an effective framework that can determine whether the act of Cyberwarfare is justified. These criteria require that Cyberwarfare may only be invoked “against entities that endanger or disrupt the well-being of the Infosphere” or “to preserve the well-being of the Infosphere.” Taddeo proposes a strong framework for determining whether Cyberwarfare is just, and such a framework can likely be well integrated into the workflows/processes that constitute the ethical analysis of traditional.

We can effectively apply Taddeo’s framework for analyzing Cyberwarfare and quickly determine that the currently existing conflict and continued cyber-enhanced/cyber-enabled retaliation between the two countries is not just. The first principle of Taddeo’s framework which prescribes that such an act may only be invoked against an entity that “endanger[s] or disrupt[s] the well-being of the Infosphere” emphasizes proportionality. This means that the first principle prioritizes the amount of good and aims to minimize harm. The Cyberwarfare between Iran and Israel continues to escalate. Not only is critical civilian infrastructure being targeted, but even health systems such as the Hillel Yaffe Hospital in Hadera are being targeted. This could have direct impacts on the livelihood of civilian/non-combatant populations and blurs the lines between Cyberwarfare and its traditional counterpart. This inarguably could cause a great degree of harm compared to the amount of good. The second principle emphasizes the preservation of the Infosphere and the informational entities that reside within it. This conflict has placed no

emphasis on preservation whatsoever and consists of incredibly haphazard retaliations that exist to simply cause destruction; therefore, as prescribed by Taddeo's framework, the conflict between Iran and Israel is not just.

Kantianism emphasizes aligning one's actions and intentions with a categorical imperative to be good, or to be just. By viewing the conflict that continues between Iran and Israel through such a deontological lens, we can effectively determine that there is no observable good that resides within the intentions of either side; therefore, as prescribed by Kantianism, we cannot consider this conflict to be just.

As observed by this case analysis, both Boylan and Taddeo proposed various issues that are present in the currently implemented JWT, which has some significant shortcomings about how it can be applied to Cyberwarfare and other non-traditional methods of warfare. Taddeo presents a strong framework that effectively addresses the issues proposed by Boylan and strongly aligns with the deontological positioning/reasoning proposed by Kant. By applying both positions/viewpoints to the conflict that exists between Iran and Israel, we can make a much stronger determination of whether these conflicts are indeed, just. There are still some valid arguments that may be presented against this deontological positioning, such as a Utilitarian viewpoint which might argue that Cyberconflict is a more ethical solution compared to the alternatives such as more traditional warfare. Although this is true, in the case of the conflict between Iran and Israel, there is no longer a focus on minimizing suffering, but more so what appears to be an emphasis on the maximization of suffering.