Case Analysis 6: Is the Cyber War between Iran and Israel a Just war?

Cyber Warfare is the use of Information Technology against another nation-state to disrupt its activities for military purposes. Iran and Israel have conducted cyber attacks on the opposing nation-states that seem to have little to no military purpose. Cyber Warfare tactics being used by both nations are driving the world toward a dangerous new norm on how nations conduct war. In this Case Analysis I will argue that Deontology shows us that the cyberwar between Israel and Iran is not just because attacks have escalated to include attacks on infrastructure that effect the civilian population and vice versa. The attacks on these systems could eventually lead to the loss of human life. The cyber war between the two countries seems to not deter the escalation to traditional war. This is setting a poor "universal law" for cyber warfare. That it is okay for cyber warfare to be used for escalation and not as a deterrent. It is just trading blow for blow. An eye for an eye leaves the whole world blind. If we make exceptions to attack the critical infrastructure of other countries that directly affect civilians, then we are setting a principle that if blood is not shed, then everything is free game. The conflict between Iran and Israel has seen attacks on infrastructure that are potentially life threatening. With each retaliatory attack between the two countries there is a rising threat to the civilian population. Both countries have launched attacks again infrastructure that seem to have no military purpose such as hospitals and public gas stations. Though no one has been killed in these cyber-attacks, they become increasingly dangerous to the public of both countries. But what happens once life is lost, and tensions erupt into physical confrontation?

Tension between Israel and Iran have always been high. However, in the recent decades we have seen the conflict between the two countries take a new form. The information revolution has brought with it many changes, including the way in which war is conducted. One example of this would be the computer worm Stuxnet. Understanding Stuxnet and its malware predecessors' sheds light on

the escalation of cyber warfare between the two nation-states. The United States and Israel are believed to be responsible for this attack. Along with Stuxnet, there is Duqu and Flame. The purpose of this malware varies in its intentional use. Flame and Duqu gathered information in secret and was a form of reconnaissance for the Stuxnet attack. Stuxnet worked by damaging centrifuges used by Iran to enrich uranium. The practice of uranium enrichment is common practice in nuclear power plants, which was Iran's stated reason for the program. Information gathered through Duqu and Flame uncovered that Iran was enriching uranium far beyond what was needed for a power facility. The uranium was being enriched into levels that could be used for nuclear weapons, which is far beyond the threshold needed for a powerplant. In "Can there be a just cyberwar?" written by Michael Boylan he writes of "Target distinction." (Boylan) Target distinction is important during war, this is what is considered before an assault is launched. "*ius in bello* the warring factions may attack military targets OR civilian targets that are enabling the military to fulfill its mission." (Boylan) This was the intention of Stuxnet. The attack can be considered successful and just as it delays the enrichment program by at least 2 years and resulted in no loss of life. It also did not impact infrastructure that directly affects civilian life. This in its own can be just and a means to an end. It can be considered a successful attack of Cyber Warfare because it minimized collateral damage and did not cause any harm to the public of Iran. Boylan talks about collateral damage when it involves "dual use infrastructure" (Boylan). As the war escalates between the two countries, there is an increase in collateral damage which increases the risk to civilians and non-war parties.

Iran and Israel have been targeting infrastructure that is critical to its citizens. "Shortly after the outbreak of the coronavirus pandemic, Iranians attacked the systems at six water and sanitation facilities in Israel." (Amer) This attack was dangerous, disrupting sanitation facilities and water supplies could have catastrophic effects on civilian populations leading to thirst, disease and other sever outcomes. This seemed to have no strategic military objective. There has been an increase in the attacks

on “dual use infrastructure” (Boylan) , that is infrastructure utilized by both military and civilian population. Iran launched an attack on Hillel Yaffe Hospital in Holdera. The attack could have had deadly consequences on the civilian population and targets an area of infrastructure. What strategic military purpose did this attack have? None it seems. This was in response to an attack from an unknown origin that targeted Iranian Railways and canceled many trains. It brings us also to “Attack and response” (Boylan) which was highlighted in Boylan’s paper. “Country X launch a cyber-attack on country Y and country Y retaliates with a cyber-attack against country X of the same scale.” In the cyber war between Iran and Israel we see a consistent back and forth and escalation of the attacks seeming to bleed more into infrastructure that impacts civilians. Starting from Stuxnet and the attack on the Iranian uranium enrichment program, escalating all the way to an attack on Hillel Yaffe.

Deontology and the categorical imperative show us that we need to be moral in all our affairs. Kant says to “act so that the maxim of your action can be willed as a universal law.” (Muscente and Kant) Iran and Israel’s cyberwar can not be justified by the way it is conducted. The escalating attacks on dual use infrastructure will eventually lead to the loss of life or traditional warfare. Can a just cyber war really be a consistent “tit for tat”? What is the difference between bombing a hospital full of civilians and completely taking it offline causing a loss of life? Isn’t poisoning a countries water supply with contaminants the same as manipulating its water treatment facilities with malware causing water to go untreated into civilian homes? There are harmful consequences to civilian life and no military strategic purpose that can justify these actions. In traditional warfare, the minimization of civilian casualties is always critical to consider before carrying out an assault, but that seems to not be the case when it comes to the realm of cyber warfare. Its difficult to say that the attacks are moral even if life is not lost. This will eventually be the reality of these attacks if they continue to involve infrastructure that impacts the civilian population. Iran and Israel can not set a “Universal Law” for cyber warfare that involves the inconsideration for the massive amount of damage they can inadvertently do to the public.

When discussing if the cyber war between Israel and Iran is justified, we can also turn to Mariarosario Taddeo's "An Analysis for a Just Cyber Warfare". Taddeo talks about "discriminations and non-combatant immunity" (Taddeo) which in the matter of warfare is the ability to target and avoid as much harm to civilians as possible. Its easy to see how the current state of attacks between the nation-states are failing in this matter. Cyber attacks that target civilian infrastructure such as ports, railways and hospitals show a lack of caution when effectively selecting targets. There is no discrimination in these attacks. Iran was subject to a cyber attack from an unknown source that effectively shut down gas stations across the country. No nation has come forward claiming responsibility for the attack, but this did cause widespread disruption at the pumps for Iranian citizens. Cards for subsidized gasoline were unusable and it caused a massive backlog of customers throughout the country. Attacks like this can affect the livelihood of noncombatants. Though we can't say this was an act of cyber war since no specific nation has claimed responsibility, it is attacks like this and the one on the hospital Hillel Yaffe that shows poor judgement in discriminating against targets in cyber warfare. For the cyberwar between the two countries to be just, both nations would need to actively engage in better methods of discrimination when selecting targets and take caution when selecting dual purpose infrastructure as a target since this can have direct consequences on citizens not involved in the military operations.

Taddeo also works on setting principles for a just cyber war by applying the principles of Just War Theory. One of these principles, "Cyber War ought to be waged to preserve the wellbeing of the infosphere" (Taddeo). The attacks between the two nations don't really work towards this goal. There is no preservation of the "Infosphere" (Floridi) when the attacks are waged. Instead, the attacks between the two countries are simply being used as a means of assault against each other rather than trying to preserve the current state of the "Infosphere". (Floridi) This brings us to a second principle that Taddeo talks about which is "Cyber War should act only when some evil has been or is about to be perpetrated with the goal of stopping it" (Taddeo). It is easy to argue that the Stuxnet attack followed this principle.

The attack was precises, with a clear goal in mind to stop the uranium enrichment program as it could have had catastrophic consequences if weapons were made. The attacks following Stuxnet fall short of this. They differ because don't have a clear goal of stopping an "evil". Iran launched attacks on water treatment facilities in Israel, and in retaliation Israel attacked Bandar Abbas, and Iranian port. This attack was responded to with the cyber assault on Hillel Yaffe hospital. The three attacks mentioned were not used to prevent any kind of evil action and only carried out in retaliation. These attacks did not follow the principles set forth by Taddeo and Thus is an unjust war.

Analyzing this with Kant's theory of Deontology and the categorical imperative shows the immorality between the attacks. Partnered with Toddeo's Principles for a just cyberwar, the currant state of attacks between the two countries do not work towards building universal laws for cyber warfare that is morally good. "The choice to resort to Cyber Warfare is furthermore justified if it allows a state to avoid the possibility of a traditional warfare." (Taddeo) In this case, we see that the attacks on civilian infrastructure do not avoid traditional warfare but instead are escalating to a point where traditional warfare may be the outcome. There is no clear goal in mind for preservation or to stop a type of evil action. This can have deadly consequences for either nation should the attacks cripple critical infrastructure causing harm among its citizens and the defending country launches a traditional assault in retaliation. The war between Israel and Iran can not be justified if the path of escalation continues and the actions show us that no target in cyber warfare is immune to attack. Israel and Iran can't make exceptions when choosing targets either, for if one country chooses a target with no strategic purpose, and does to simply out of retaliation, It sets the universal laws for cyber warfare to be based on retaliation and destruction rather than preservation of life. Preserving human life, and de escalating tension should be the goal in cyber war. By following Taddeo's principles, Deontology shows us that a just cyber war would be one that avoids damage to the public. If acts of cyber war are used to avoid an evil, and have a clear goal of this, like stopping the creation of a nuclear weapon, it can be considered

moral and just. Deontology would show that the maximum effect should be to de escalate and not provoke or retaliate.

To conclude whether the cyber war between Israel and Iran is just we need to consider how the attacks are leading to an escalation between the two nations. The lack of target discrimination, distinction and the growing disruption to civilian life makes this, in my view, an unjust war. When cyber-attacks are used, they should avoid collateral damage as much as possible. With Stuxnet, the attack had a clear goal to stop a growing evil and was direct with no collateral damage to the public. This should be the universal law we set forth for cyber warfare, where we use cyber-attacks as a means of preservation and not a means of assault. Where attacks must be direct, and not blur the lines between state infrastructure and civilian infrastructure. Using Taddeo's principles for a just cyber war we can set a standard that only uses cyber warfare as a necessary means to avoid traditional conflict. The maximum of cyber warfare tactics needs to embrace a means to an end and not harm the population. Kant makes the argument to "do unto others as you would have them do unto you." (Muscente and Kant) At this rate, we are just opening the world of cyber warfare to involve everyone and everything which is deadly and will ultimately lead to human lives lost or traditional warfare. We need to use cyber warfare as a tool to avoid the disruption of civilian life and infrastructure and not used to cripple it and escalate to bloodshed.

Case analysis 6 works cited.

Amer, Adnan. “The Cyberwar between Israel and Iran Is Heating Up.” *Middle East Monitor*, 8 Nov. 2021, www.middleeastmonitor.com/20211108-the-cyberwar-between-israel-and-iran-is-heating-up/. Accessed 6 Apr. 2023.

Boylan, Michael. *Can There Be a Just Cyber War?* Sept. 2013, hdl.handle.net/2115/54138.

Floridi, Luciano. *The Fourth Revolution : How the Infosphere Is Reshaping Human Reality*. Oxford, Oxford University Press, 2014.

Muscente, Kailee, and Immanuel Kant. “Categorical Imperatives and the Case for Deception: Part I | IRB Blog | Institutional Review Board | Teachers College, Columbia University.” *Teachers College - Columbia University*, 13 July 2020, www.tc.columbia.edu/institutional-review-board/irb-blog/categorical-imperatives-and-the-case-for-deception-part-i/.

Taddeo, Mariarosaria. *An Analysis for a Just Cyber Warfare*. 2012.