Shacara Pitre

PHIL 355E

April 6, 2022

Case Analysis on Cyberconflict

In both articles assigned, they discuss how Iranians were unable to get gas due to a cyber attack interfering with gas stations. It was caused by a computer glitch in a major supply network. There was a cyberwar going on between Israel and Iran that caused this to happen. The President of Iran, Ebrahaim Raisi, even confirmed this by saying that this incident showcased "readiness in the field of cyberwar" (Silva, Collier, and Reuters, 2021). The cyberattack on Iranian gas came just weeks before the second anniversary of deadly protests over high gas prices. Since Iran's digital infrastructure relies on outdated Western software, they are more vulnerable to attacks. They believed the attacks were coming from either the United States and/or Israel, but it was not confirmed. There have been many back and forth attacks between Iran and Israel. For instance, during the pandemic, "Iranians attacked the systems at six water and sanitation facilities in Israel" (Silva, Collier, and Reuters, 2021). To combat this, Israel launched a cyber attack on computer facilities at Iran's largest port. There was even an attack on the Iranian Railways computers that canceled thousands of trains, which was believed to have been Israel. In this Case Analysis, I will argue that confucian shows us that the cyberwar between Israel and Iran is just because it tells us how to live our lives based on the overall path we walk, not by individual choices. They are simply trying to protect their respective countries from overall harm regardless of the outcome.

In Boylan's article, he starts by explaining the difference between cyber sabotage and cyber warfare as "a matter of degree". There is debate between whether or not cyberwarfare can

be justified. Also, questions have been raised about what is actually considered a war? Cyber warfare differs from traditional war because you do not always know who starts it and could come unexpectedly since it is on the internet by someone working against a government or military from within. Viruses, worms, and malware are among the attacks that occur via the internet by cyber criminals.

In Boylan's article, he recognizes that the idea of warfare needs to be expanded to include cyber-related attacks. To clarify, he states "...in the case of cyber-warfare we should move away from the at-fault liability mindset that presently exists in just war theory to one of strict liability" (Boylan). Since war is branching out from the traditional tactics, we need to be aware of other avenues for attacks, such as cyber attacks. It is important to look at the effects of these cyber attacks as well to consider if they are going to be harmful to people or just to infrastructure. Cyber warfare can be unethical depending on how a group goes about it, but it can also be justified depending on the reason and the effectiveness of it.

In terms of Confucian, cyber warfare is considered ethical if it is done for the right reasons. It tells us that we should not simply do what we are told just because someone who is a higher authority says to. The cyber war between Israel and Iran can be ethically justified because their back and forth attacks are meant to defend their country. It is not to cause intentional harm to another country. In other words, it is like if you come at me, I will come at you even harder so that it won't look like you can keep getting away with it.

That is exactly what these two countries were doing. The cyber attack that Iranians faced that involved a disruption at gas stations was meant to hurt their systems. It was believed to be anti-Iranian forces. One reason why the cyberwar between Israel and Iran is a just war is because it did not cause any physical harm. Israel only meant to impact systems in order to get their point

across and not cause any collateral damage. Even the Stuxnet worm that was used to infect software of industrial sites in Iran was for the right reasons.

The whole idea of Confucian is about stepping out of what a higher authority tells you to do and to do the right thing. This ethical perspective would have thought the cyber war between Israel and Iran was just because these cyber attacks are used as an alternative to prevent chaos and the possibility of leading into an all out war. The attack was for a political motive or gain, which shows that it was only meant as a preventative measure to protect the other country. Furthermore, it is important that countries understand the concept of cyber warfare, so that they are not blindsided to these kinds of attacks. Overall, Boylan's purpose in this article was to explain that cyber warfare should be included in the rules for war because times are changing and we need to know what to expect.

In Taddeo's article, he discusses the ethical side of cyber warfare along with if Just War Theory (JWT) is a "necessary but not sufficient instrument for the ethical analysis of CW". Cyber warfare is different from the traditional aspects of war, which is more violent and destructive usually involving human lives. For instance, Taddeo states "CW may involve a computer virus able to disrupt or deny access to the enemy's database, and in so doing cause severe damage to the enemy without exerting physical force or violence". This shows that cyberwarfare can be just because it is not using violence to solve their problems. Instead, they use tactics to get their point across.

However, cyberwarfare should still be taken just as seriously as traditional war because there are more angles that can be used since the internet is endless with possibilities. It could be even more violent and destructive if it gets out of hand. Taddeo goes on to talk about Just War Theory and how it relates to cyber warfare. Just War Theory can be defined as "war as to a

violent and sanguinary phenomenon, declared by states and their official leaders and waged by military forces" (Taddeo). War as a last resort, more good than harm, and of non-combatants immunity are three issues that are related to this theory.

First, war as a last resort states that "a state may resort to war only if it has exhausted all plausible, peaceful alternatives to resolve the conflict in question, in particular diplomatic negotiations" (Taddeo). This shows that in relation to cyber war, it is not intentionally trying to cause harm. It starts off with tactics to get their enemies attention, but not enough to cause physical harm to anyone. Second, more good than harm states "before declaring war a state must consider the universal goods expected to follow from the decision to wage war, against the universal evils expected to result" (Taddeo). In other words, this is looking into worst case scenarios in the sense that before they declare war, they need to look at all angles and to see if it needs to come to it.

Third, non-combatant immunity "refers to a classic war scenario and aims at reducing the bloodshed and prohibits any form of violence against non-combatants, like civilians" (Taddeo). In other words, cyber warfare does not have the goal of causing any harm to anyone. It is about making their point across without using violence. When it comes to Confucian, cyber warfare is needed because if we just stand idly by and let these attacks happen, then we are part of the problem. Cyber attacks occur because they are a nonviolent way of getting a point across. With Confucianism, these cyber attacks are a way to resolve a problem that goes against the traditional way.

It is about staying on the right path, but also not just standing by if you see something wrong. The cyberwar between Israel and Iran is a just war because Israel and Iran each had their own reasons for their respective cyber attacks. Cyberwarfare is not a bad thing when it comes to

the grand scheme of things because it is not causing any physical harm to people. More importantly we should consider the repercussions of what could happen if these cyber tactics did not occur. We would have a far greater problem on our hands if we did not stop the production of nuclear weapons or other things that could be used for an all out war.

In conclusion, the cyber warfare between Israel and Iran is a just war because there is always a greater reason for these cyber attacks that we need to look at. It is important that they are looked at from an ethical view because it demonstrates that cyber warfare causes more of a good outcome than a bad outcome in the long run. Some may argue that cyber warfare causes harm to infrastructure making it seem like it is bad overall. However, they are not looking at the bigger picture meaning that even though it may harm certain aspects of a country, it is still not causing mass destruction like a traditional war. Confucianism is a perfect ethical tool to use here because it is about walking the right path regardless of what a higher authority says. If someone is doing something wrong, then they need to be called out regardless if they are a political figure, parent, etc. This module has opened my eyes to a new view of cyber warfare. I always thought that it was a bad thing, but now I see that there can be good that comes out of it.