Case Analysis on Cyberconflict

Kyle D. Reinert

Old Dominion University

Author Note

This paper was prepared for Cybersecurity Ethics (PHIL355E), taught by Professor Montoya.

**Case Analysis on Cyberconflict**

Cyber war has given a bigger platform to countries that might not be able to execute the traditional warfare of the past. The tension between Iran and Israel is only getting more robust with each cyberattack performed on either end. Israel has more of an edge with its cyberwar capabilities with more deadly attacks. Still, Iran is improving their cyberwar capabilities and is a threat that can hinder Israel's technical capabilities and economy. Iran's nuclear facilities, gas stations, and transportation services being attacked by Israel cause issues for those living there; Iran is reactive with its attacks on Israeli hospitals, electrical networks, and internet servers. In this Case Analysis, I will argue that contractarianism shows us that the cyberwar between Israel and Iran is not just because it is redundant and continues a cycle of hatred toward one another when neither side wants an all-out confrontation.

Cyber warfare is an entirely new style of war that has not been seen in history books. Instead of traditional warfare where a country must physically go into foreign territory, someone can now orchestrate an attack from their homeland and cause damage to another country. However, how extreme can these cyber-attacks be? It is seen that cyber warfare can have an influence on nuclear facilities, electrical grids, hospitals, and economies from the actions of Israel and Iran. Who can say they cannot cause a nuclear meltdown or another strategy that can cause an extreme impact on human lives? Michael Boylan's "Can there be a Just Cyber War?" explains that the rules regarding cyber warfare have not been recognized internationally.

Michael Boylan explains that the last time the Geneva Convention was updated was in 1949, with three precursors that also justified their eras. Innovations of war should call for updated and improved guidelines for today's new era. It currently stands that there is no recognized compensation for the lives and property loss in a potential incident, like how the United States struggled with compensating families of the lives lost in 9/11 since an event like that was unprecedented. Rules on war need to be expanded and agreed upon for a just war to be accepted to create a better world. Boylan brings up a concept of a new mindset that "would look at the damage caused by some actor and move it into international civil law." This concept aligns very close to contractarianism as it will apply a social contract to everyone to create a better life for all by trying to "settle acts of aggression" and prevent unnecessary carnage.

Cyber warfare does have its upsides when compared to traditional war. Cyber war can be more selective to who and what it affects, as it does have the potential to be lethal to human life; it can also be very harmless in determining an attacker's intentions. Mariarosario Taddeo's "An Analysis of Just Cyber Warfare" mentions a principle of "more good than harm" to describe a just war that could be considered as something that must be done for the greater good. In contractarianism, this principle can be applied because only those following the social contract would be protected from the consequences of disobeying an agreement made by everyone. This can also relate to another principle Taddeo mentioned, that if "any entity that endangers or disrupts the well being of the Infosphere loses its basic rights and becomes a licit target."

Taddeo's principles do not justify the Israel and Iran cyber conflict. Israel nor Iran are entities that must be stopped for the greater good. The conflict between these two countries is more of a constant reactive issue, I will attack you because you attacked me, that neither truly wants to confront the other. What they are doing is constantly harming themselves by not trying to pursue peace with one another and continuing this cycle of hate that will never find an end to this cyber war until much more extreme actions will be executed to prevent the other country from reacting. Cyber warfare is definitely a better alternative because it can be non-violent and non-physical that can possibly not affect humans, but it can be as devastating as traditional warfare and easier to do.

Cyber-attacks have been causing issues with more than just the government but for citizens living within. The cycle of hatred that I am speaking of exists in any type of war because there will always be victims that have their lives and freedoms looked over. The more cyber-attacks occur, one side will try to one-up the other, which will cause some trouble that Boylan mentions. That is because we do not have rules with the limitations of the actions that those conducting cyberwarfare can and cannot make. There are no commonly agreed rules that Israel and Iran must follow, or any other country in that matter, that do align with contractarianism.

Neither Israel nor Iran is more special to other or any other place. We all live in this world and would find attacks on ourselves inconvenient, so why would doing it to someone else be right? As Iran improves with its technological advancements, it might start testing out different cyber warfare methods that could result in a more dangerous situation that might have Israel go to further measures or vice versa. There is no international agreement on the limitations of cyber warfare that could officially define how it can be considered just or not, which puts it as questionable. Using contractarianism can help determine if it is just or not. It is an agreement that should be applied to everyone and will make everyone's life better by limiting the potential carnage that cyber warfare can become. As the situation between Israel and Iran stands with no official rules for their war, it currently is unjust until everyone can determine what is right or wrong until it is too late.