Alanna Richerson

6.4 case analysis

In the cyberwar between Israel and Iran both have targeted one another's networks and infrastructures with a cyberattacks that are complex. Israel has allegedly orchestrated numerous cyberattacks against Iran one of the most notable attacks they have launched is the Stuxnet virus. The Stuxnet virus was deployed with intentions of disrupting Irans nuclear program. Seeking out retribution Iran has also allegedly produced numerous attacks in retaliation against Israel operations. Both are stated as allegedly due to neither Israel nor Iran recognizing these attacks. During Israel vs. Iran battles may escalate into the need for military interference from departments outside of cybersecurity due to these attacks targeting the security measure which is most vulnerable, so the attack does a large amount of damage in comparison to the minuscule amount of resources the victim has available. In this Case Analysis, the object of it is to examine the ethical tool the Just War Theory to provide insight into the morals of the Israel vs. Iran cyberwar.

One of the main focuses of Boylan's work is consequentialism. Consequentialism is an ethical theory which that analyzes how moral an action is based on the outcomes or consequences. In the position of consequentialism, the outcomes and consequences must be one of the best possible to be considered morally correct. When using consequentialism, the actions that each Iran and Israel have taken during this war can be analyzed using the outcomes that have been produced. Consequences can be used to measure morality in Israels usage of cyberattacks such as Stuxnet to disrupt Iran's nuclear operations. The argument for this may be that Iran's goals for their nuclear program may have been severed. This would be seen as morally justified due to this move causing Iran's nuclear capabilities to not be able to multiply and thus possibly halting a conflict between regions. Concerns are raised though with consequentialism when the unintentional consequences are considered. The is increased concern of revenge and intensification of war that comes with the increase of weapons such as Stuxnet because not only could these weapons make international relations unstable. Consequences are both immediate and long term so while the immediate effect of the Stuxnet attack may be the disruption of Irans nuclear programs in the long term it may lead to increased security, and a wider area of destabilization due to a higher risk of retribution.

Cyber sovereignty is a main concept in Taddeo's work meaning the rights of states to govern/control their own cyberspace. Cyber sovereignty discusses internet activities and the country's authority over regulation while taking into consideration defense of critical infrastructure, law enforcement, and cyber threat protection. During analyzation cyber sovereignty is utilized to depict those actions of Israel and Iran and how much they respected the others cyber sovereignty. On one hand, the unauthorized access of Iran's cyberspace and critical infrastructure interference during the Stuxnet attack may be viewed as a violation of Iran's cyber sovereignty. On the other hand, the cyber operations Iran is using to retaliate against Israel can be seen as a violation of Israel's cyber sovereignty. While using cyber sovereignty as a method for ethical analysis evaluation of the actions taken by Israel and Iran can be evaluated by how much they follow international laws and national sovereignty. If we use this point of view to analyze then the cyber attacks deployed by Israel can be seen as unethical due to the violation of Iran's authority rights an in the domestic affairs of other states, they breach the norms of non-interference. Same goes for the retribution cyber operation Iran is utilizing if the operations undermine the stability of the region or cause tensions to escalate their methods can also be viewed as unethical.

Conclusion

In conclusion, The Just war theory displays how complex the ethical considerations play a part in modern warfare especially when utilizing it to evaluate the Israel vs. Iran attacks. Distinctions that were traditionally utilized to differentiate attackers and civilians have begun to cloud the principle of using discrimination which worsens the risk of civilians getting caught in the crossfire. While using ethical reasoning it highlights the need for continuous modification and adaptation of these ethical frameworks to fit into how sophisticated modern warfare is. When evaluating the justices of cyber operations in the 21st century a critical tool that is utilized is ethical analyzation. To effectively address the ethical problems that arise with warfare in the 21st century a variety of considerations should be taken into place to supplement the analysis such as diplomacy, international laws, and the innovation of technology over the years.