Olivia Diaz

Phil 355E

7/29/2023

Case Analysis on Cyberconflict

Latest incidents have significantly disrupted Iran's gas stations since the cyberwar involving Israel and Iran becomes more intense. The two parties participated in significant cyberattacks on their counterparts, which resulted in targets from all individuals. The latest hack by Iran against Israel's Hillel Yaffe Hospital has major repercussions, forcing medical facility personnel to operate manually and perhaps putting Israeli individuals in peril. In consequence, it was assumed that the Israeli hack on Iran's gasoline distribution system was punishment for the hospital strike, signaling an intensifying war.

The two nations are susceptible to the possibility of financial and technological harm brought about by advanced computer viruses as the cyberwar intensifies. Though Israel might have the upper hand during this cyberwar, Iran is developing its strengths and gaining new skills Which renders it better able to counter Israeli strikes. In this Case Analysis, I will argue that the virtue ethical tool shows us that the cyberwar between Israel and Iran is not just because of the growing harm done to innocent civilians and the possibility for negative outcomes notwithstanding the advances in technology.

Michael Boylan examines the idea of the theory of just war in the setting of cyberwarfare in his piece titled "Can There Be a Just Cyber War?" The premise of "Jus in Bello," tackles moral behavior of conflict after it starts. It constitutes among of the main ideas he examines. Boylan emphasizes the necessity of balance and discriminating in the employment of force throughout conflict. He stresses that all the damage done to populations needs to be reduced while ensuring that armed forces should be proportionate with the desired goal.

The growing harm done to innocent people, including the online attacks against gas stations and medical facilities, presents moral issues when the Jus in Bello concept is applied to the instance of the cyberwar involving Israel and Iran. Innocent citizens that don't take part in the war are immediately impacted by the suspension of crucial amenities such as medical and gasoline supplies. These kinds of assaults violate the concept of equal treatment since they put individuals in danger and may have significant repercussions.

Furthermore, concerns regarding balance are raised by the cyberwar's amplification and rivalry strikes by each party. The employing of cyber force must be calibrated and proportionate to the damage already done or anticipated to be done. The evidence in this case, nevertheless, points to an absence of a proportionate reaction since attacks appear to have escalated and innocent people have been targeted on the two parties.

According to the virtue ethical tool, an analysis regarding the case's acts shows they are not consistent with virtue traits. Fairness, knowledge, and empathy are just a few examples of the ethical traits that are emphasized in virtue ethics. Virtuous behavior in cyberspace warfare includes seeking out methods that are peaceful, using caution while using pressure, and placing the safety of innocent citizens above everything else.

Yet the intensifying internet warfare among Iran and Israel shows an absence of moral conduct. Retaliatory assaults are being launched by both sides, disrupting crucial services for civilians. A emphasis on vengeance instead of noble ideals is suggested by the desire of more security breaches and possible intensification.

This research makes it clear that the ongoing cyberwar among Israel and Iran is unjust because it infringes fundamental Jus in Bello rules of ethics and opposes moral behavior. A detrimental strategy to combat is evident from the growing effect on targets who are civilians, the absence of balance, and the punitive responses.

Prioritizing political approaches and the amicable settlement of disputes in this situation would have proven the best course of action. Cyberwarfare should only be used as a last ditch effort when every other tranquil option has been thoroughly explored and has the possibility to hurt people and prolong the dispute. Instead of launching cyberattacks, the two sides could have held substantive discussions and looked for areas of agreement.

The virtue ethics tool and Michael Boylan's principles are used to examine the cyberwar involving Israel and Iran, emphasizing the unfair aspect of the dispute. Issues about ethics are raised by the effect on the civilian population and the absence of moral behavior in the growing number of cyberattacks.

The main idea of Mariarosaria Taddeo's piece, "An Analysis for a Just Cyber Warfare," is the moral study of cyber warfare (CW) and its connection to information ethics and just war theory (JWT). The purpose of this study is to provide a moral basis towards the development of norms to govern this type of conflict in order to solve the moral quandaries regarding cyberwarfare. The informative character of cyberwarfare, plus the difficulties that occur when using the just war theory to handle its innovative elements have been taken into account in Taddeo's study.

The circumstances involving the cyberwar among Israel and Iran may be examined using Taddeo's classification of cyberwarfare and taking into account the ideas of just war theory and information ethics. The intellectual structure of cyberspace, where both tangible and intangible things interact and have the same worth, serves as a factor to take into account.

Israel and Iran executed cyberattacks in this situation, focusing on one anothers cyber infrastructure while operating inside an informative context. Since cyberwarfare can entail acts that impair or manipulate adversary assets without inevitably causing damage to people, the amount of force can differ. Yet, the generality of cyberwarfare poses moral dilemmas since such attacks have the capacity to turn aggressive, seriously causing harm to society.

According to virtue ethics, judging what was committed throughout the cyberwar involving Israel and Iran requires assessing the morality of the participants and their commitment to virtues. Knowledge and empathy are qualities that are highlighted by virtue ethics. The moral thing to do might be to exercise patience and prioritize compromises while taking into account the risk of damage to people.

According to the findings of the research and evaluation, using the concepts of information ethics and just war theory to control cyberwarfare might be considered the correct decision to pursue in this situation. The two sides should've made an effort to limit the amount of force used and prevent needless injury to citizens while upholding the norms of balance and impartiality.

The distinctive elements of cyberwarfare, which are both material and intangible things are just as important, may also be addressed by adopting information ethics as a component of the moral structure. This involves creating a moral evaluation that takes into account the unique aspects of cyberwarfare yet being compatible with the moral structure often used to analyze conventional combat.

We could additionally evaluate the instance of the cyberwar among Israel and Iran if we employ Mariarosaria Taddeo's classification of cyberwarfare. The establishment of digital tools attacking one another's assets across the digital realm constitutes cyberwar, which has taken shape inside the informative context. Cyberwarfare is shown by this kind of conflict in which all elements cohabit, and levels of aggression can fluctuate. The key characteristic of cyber warfare is its capacity to develop from peace to increasingly lethal kinds, harming armed forces and the public significantly.

To successfully traverse the intricacies of cyber battles and provide an equitable and morally acceptable strategy for combat, it is essential to emphasize characteristics like knowledge, diligence, and kindness.

In Summary, to Michael Boylan's just war theory, Mariarosaria Taddeo's analysis, and the virtue ethical tool, the cyberwar between Israel and Iran is unfair. The escalating damage brought about by cyberattacks affects defenseless populations, which shows an absence of morality and balance. The dispute worsens because of the two parties' reactive measures, which are against fair warfare ideals.

Virtue ethics requires gentle, compassionate action, which is very clearly absent during this cyberwar. Cyberwarfare rules need to be governed by information ethics and the just war theory, which ought to provide peaceful alternatives to cyberattacks which hurt all human beings that are involved.

The subject matter emphasizes the necessity regarding a moral structure for cyberwarfare. Which places a focus on finding viable alternatives and safeguarding the well-being of society as a whole. Legislators and philosophers should think about larger ramifications and seek to resolve cyber disputes in modern times in a reasonable and compassionate manner.

References

Abu Amer, Dr 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/.

Boylan, Michael. *Can There Be a Just Cyber War?*

Da Silva , Chantal, et al. “Cyberattack Blamed as Iran Gas Stations Hit with Major Disruptions.” *NBC News*, 26 Oct. 2021, www.nbcnews.com/news/world/cyberattack-blamed-iran-gas-stations-hit-major-disruptions-rcna3806.

Taddeo, Mariarosaria. “An Analysis for a Just Cyber Warfare.” *4th International Conference on Cyber Conflict*, 1 Jan. 2012. Accessed 30 July 2023.