Cameron Cassani

PHIL335E

November 12th, 2023

Analyzing the Israel-Iran Conflict Through a Confucian Lens

Introduction

In the ever-evolving landscape of international relations, the domain of cyberwarfare has emerged as a critical battleground, exemplified by the intensifying cyber conflict between Israel and Iran. This digital warfare has transcended traditional geopolitical boundaries, introducing a new era of conflict marked by sophisticated cyberattacks targeting essential national infrastructures and critical state assets. The Middle East Monitor and NBC News articles provide insightful details into specific incidents that have defined this cyber conflict. These cyber operations are not isolated incidents but rather reflect a broader geopolitical struggle between the two nations, each justifying its cyber offensive as a measure of defense or retaliation against the other. The complexity of these incidents lies not only in their technical sophistication but also in the moral and ethical dilemmas they present. Through the lens of this ongoing conflict, the intricate web of motive, action, and consequence becomes evident, challenging traditional notions of warfare and national defense.

This Case Analysis aims to dissect this modern battlefield using a Confucian ethical framework. Confucianism, with its emphasis on moral integrity, societal harmony, and mutual respect, offers a unique perspective in assessing the justness of cyber warfare. By examining the actions of both Israel and Iran in this digital conflict, this analysis will argue that, according to Confucian ethical principles, the cyberwar between these two nations is not just. The reason lies in the fundamental breach of Confucian values: the disruption of societal harmony, the

undermining of mutual respect, and the failure to adhere to the ethical conduct prescribed by Confucian teachings. Therefore, this analysis will contend that the cyberwar, in its current form and manifestation, deviates from the path of righteousness and justice as delineated in Confucian philosophy.

Analysis using Boylan's Concepts

Michael Boylan's framework for understanding the ethics of warfare, particularly in the context of modern conflicts like cyberwarfare, is pivotal. His approach examines the traditional just war theory, which includes principles such as legitimate authority, just cause, right intention, probability of success, last resort, and proportionality. Boylan extends these principles to cyber conflict, emphasizing the need to evaluate digital warfare's moral imperatives and consequences.

Applying Boylan's framework to the cyberwar between Israel and Iran, several ethical considerations arise. Firstly, the principle of cause and right intention can be scrutinized. While both nations may claim defensive or retaliatory motives, the underlying intentions often seem to veer towards demonstrating power or undermining the opponent rather than addressing specific, justifiable grievances. For example, Iran's cyberattacks on Israeli water infrastructure and Israel's response with similar cyber operations raise questions about the right intention behind these actions.

Secondly, the principle of proportionality is crucial. Boylan's theory suggests that actions in war must be proportional to the achieved goal and should avoid unnecessary harm, particularly to civilians. In the context of cyberwarfare, this becomes complex, as cyberattacks on critical infrastructure can have far-reaching impacts on civilian life, potentially violating this principle.

From a Confucian perspective, the actions observed in the Israel-Iran cyber conflict fall short of ethical standards. Confucianism places a strong emphasis on 'Li' (propriety) and 'Ren' (benevolence). The aggressive nature of these cyberattacks, often resulting in collateral damage to civilian life and disrupting societal harmony, starkly contrasts these principles. In Confucian ethics, the well-being and harmony of the community are of paramount importance. The cyberwar tactics employed by both Israel and Iran, which risk civilian welfare and social stability, are thus seen as unethical.

Furthermore, Confucianism values' Yi' (righteousness), where actions are supposed to be morally right and justifiable. With its shadowy nature and often unclear objectives, the cyberwar challenges this notion. The lack of transparency and the potential for hidden agendas in these cyber operations raise doubts about their righteousness.

In summary, when viewed through the lens of Boylan's just war concepts and Confucian ethical principles, the cyberwarfare tactics employed by both Israel and Iran appear to be lacking in moral justification and proportionality, disrupting societal harmony, and failing to uphold righteousness and benevolence. This assessment leads to the conclusion that the ongoing cyberwar between these two nations is not consistent with the principles of a just war as defined by Boylan and is contrary to the key tenets of Confucian ethics.

Analysis using Taddeo's Concepts

Mariarosaria Taddeo delves deeply into the ethical intricacies of cyber warfare, offering a framework that scrutinizes the justifiability of actions in the digital realm. Her approach emphasizes critical concepts like the proportionality of response, the distinction between

combatants and non-combatants, and the necessity of actions taken in cyber conflicts. Taddeo's analysis is crucial in understanding the moral landscape of cyber warfare, especially in conflicts where the nature of cyber operations challenges traditional warfare norms.

Applying Taddeo's concepts to the cyberwar between Israel and Iran reveals several ethical challenges. The principle of proportionality, for instance, is a critical factor. In Taddeo's view, cyber warfare actions must be proportional to the threat and aimed at preventing harm. However, in the case of Israel and Iran, the cyberattacks often escalate beyond the immediate threat, potentially causing broader harm than necessary. For example, disrupting civilian access to essential services like fuel and water goes beyond a direct military response and enters the realm of affecting the general populace.

Another important aspect in Taddeo's framework is the distinction between combatants and non-combatants. In traditional warfare, this distinction is clearer, but in cyber warfare, the lines are often blurred. Attacks on civilian infrastructure, as seen in this conflict, directly impact non-combatants, challenging the ethical justification of such actions.

From a Confucian standpoint, these actions are even more problematic. Confucianism emphasizes the importance of 'Ren' and 'Li', advocating for actions that promote social harmony and the well-being of all. The indiscriminate nature of cyberattacks, which can affect civilian populations and disrupt societal order, directly contradicts these principles. Moreover, the concept of 'Zhong' (loyalty) in Confucianism extends to loyalty to moral principles, not just to one's state. Thus, actions in cyber warfare that prioritize state objectives over moral righteousness are viewed as unethical.

In addition, Confucian ethics stress the value of 'Xin' (trustworthiness). In the context of cyberwarfare, maintaining trustworthiness becomes challenging, especially when states engage

in covert operations that can be perceived as deceptive or underhanded. The secretive nature of cyber warfare, with its lack of transparency and potential for misinformation, undermines this Confucian value.

In conclusion, through the analytical lens of Taddeo's concepts, coupled with Confucian ethical principles, the cyberwarfare tactics employed by Israel and Iran raise serious moral concerns. The lack of proportionality, the impact on non-combatants, and the potential breach of trust all suggest that the actions of both nations in this cyber conflict fall short of the ethical standards outlined in both Taddeo's framework and Confucian philosophy. This analysis thus supports the thesis that the ongoing cyberwar between Israel and Iran is not aligned with the principles of just warfare as envisaged by Taddeo and is at odds with the fundamental tenets of Confucian ethics.

Conclusion

Overall, it's evident that the cyberwar between Israel and Iran presents a complex ethical landscape, particularly when examined through the frameworks of Michael Boylan, Mariarosaria Taddeo, and Confucian ethical principles. The primary conclusion drawn from this analysis is that the ongoing cyber conflict between these two nations does not align with the principles of a just war as outlined by Boylan and Taddeo, and it contravenes key tenets of Confucian ethics.

The actions of both countries, mainly the cyberattacks that often impact civilian populations, fail to meet the ethical standards outlined in traditional just war theory and Confucian philosophy. The lack of clear legitimate authority, the questionable intentions behind

the cyber operations, and the apparent prioritization of strategic gains over peaceful resolution exacerbate these ethical concerns.

Furthermore, this analysis opens up broader discussions on the need for an updated ethical framework that addresses cyber conflict's nuances. As nations increasingly rely on digital means for both defense and aggression, the international community faces the pressing task of establishing clear guidelines and norms that govern cyberwarfare.

In considering the wider implications, this case also highlights the growing importance of cybersecurity and the ethical responsibility of nations to protect their citizens from digital threats. The Israel-Iran conflict serves as a stark reminder of the potential for cyberwarfare to escalate and cause significant harm, underscoring the need for robust ethical considerations in the development and deployment of cyber capabilities.

In conclusion, while this analysis points towards the unjust nature of the cyberwar between Israel and Iran, it also underscores the complexities and evolving challenges in applying traditional ethical frameworks to modern conflicts. This calls for a continuous and dynamic discourse on ethics in cyberwarfare, accommodating the unique attributes of digital conflicts while striving to uphold moral principles and international norms.