6.4 Case Analysis on Cyber Conflict

Introduction

The introduction of cybersecurity has brought a new domain of conflict in warfare. Instead of nations attacking each other by just conventional means, but also unconventional. In the article “Digital Battlegrounds: Evolving Hybrid Kinetic Warfare” it introduces the term hybrid warfare. It is also known as asymmetric warfare, which is a strategy that utilizes both conventional and nonconventional tactics. Traditional methods involve physical force, while non-conventional is non kinetic. Examples of non-conventional are cyberattacks on critical infrastructures, public services and supply chains. These non-conventional attacks can have a devastating impact in a country’s economy, national security, and social wellbeing of citizens. For example, a cyber-attack on a water treatment facility can disrupt the supply of clean water, which could jeopardize public health.

The prompt for this case analysis is “focusing on the cyberwarfare actions described, considered on their own, could these actions be part of a just war, or would these actions be unjust even within an otherwise just war?”. Based on the article, it is a bit difficult to determine if the cyber actions described are part of a just war. However, in this case analysis I will argue that deontology shows that these actions could not be part of a just war because cyber-attacks lead to devasting consequences to not only a country’s overall structure but the well-being of citizens, and if the attackers are aware of the consequences, then that shows no moral intentions.

Case 1

One of Michael Boylan's concepts is the challenge of applying traditional just war theory in cyberwarfare. Before going into detail about Boylan's concept, Just War Theory will be covered. The Just War Theory is a philosophical framework that seeks to determine two aspects:

1. Jus ad Bellum: The right or moral justification for going to war (below is a set of criteria)
    - Just cause
    - Right intentions
    - Last resort
2. Just in Bello: The right conduct of war (below is a set of criteria)
    - Military Necessity
    - Discrimination: distinguishing legitimate military targets and avoiding harm to civilians

    The main goal of the Just War Theory is to help balance the protection of society and combine injustice with moral intentions, while also mitigating harm of innocent civilians both during and after the war.

    Boylan makes an argument that due to cyber-attacks anonymity and complexity; it can be complicated to apply moral frameworks like the Just War Theory. The issue of attribution is one factor to the difficulties of cyberwarfare. In the traditional realm of warfare, it is quite easy to distinguish the aggressor. However, in the cyberspace environment, it is difficult to determine and identify who the attacks are. This makes it a challenge to assess who's responsible for the attacks. Without any clear attribution, it becomes very difficult to justify a proportional response. Another factor that Boylan

empathizes with is the disproportionate impact of cyberwarfare on civilians. Physical war zones are easily distinguishable, but this is not the case for cyberwarfare. Cyber-attacks can affect civilians globally, and this raises concerns of collateral damage. In this case, Boylan raises the question if principles of jus in bello like discrimination between combatants and civilians can even be upheld.

Looking into the lens of Boylan and comparing it to this case analysis, Boylan could argue that the actions described in the article about hybrid warfare are unjust in a just war. Upon reading the article, it goes into detail about the devasting impacts cyber-warfare can have on a country's national security, critical infrastructures, and civilians. Based on the Just War theory, the idea is to protect and minimize harm on civilians. Hybrid warfare goes against those principles of Just War, which is a point that Boylan seems to be making. Cyberwarfare adds a new level of complexity it is difficulty to determine if the cyber-attack is a justifiable proportional response, because out of technicality, cyber-attack is considered non-kinetic or a physical form of force that physical harms people.

Looking through the deontology lens, it could make a similar agreement to Boylan. Looking into the actions described in the article, there are many devasting consequences that follow cyber warfare. Unfortuntatly, it heavily impacts civilians. Since deontology heavily emphasizes respecting people, it would make the case that the actions described in the article are not justified in a just war. Also, if the attackers knew that their cyber attacks could have such an impact on citizens, then that is not a moral intention, which is a major principle in deontology.

Case 2

Mariarosaria Taddeo has a similar viewpoint as Boylan. However, she argues how the Just War Theory can be applied to cyber warfare. One of the concepts that she emphasizes is the principle of discrimination. Typically, in traditional warfare there is a requirement for combatants to distinguish themselves from non-combatants. This is to ensure that civilians are not targets and harmed. However, this is where Taddeo argues that cyberwarfare makes this principle complicated to apply. In cyberwarfare, there isn't a clear physical boundary, nor clear roles on who are and not combats. Cyber attacks can affect any individual indiscriminately. A cyber attack could affect critical infrastructures that impact both military and civilians.

Taddeo mentions that for a cyberattack to be justifiable, it should not target civilians and nonmilitary infrastructure. Also, Taddeo suggests that there needs to be an ethical guideline for cyberwarfare. For the guidelines to succeed it must adhere to the principles of discrimination and prevent indiscriminate damage. Also, according to Taddeo the guidelines would need international cooperation and robust cybersecurity laws that prioritize the safety of civilians and minimize harm.

Taking Taddeo's concept in "An Analysis for a Just Cyber Warfare" and compare it to the article, like Boylan, she will agree that the actions of hybrid warfare is not part of a just war. This is because the article describes how hybrid warfare has a devastating impact on critical infrastructures, supply chains, and public services that negatively influence the well-being of innocent people. However, unlike Boylan, there is a part in the article that Taddeo will agree to.

The last two paragraphs discuss how nations should develop robust preventative measures, and strategies to mitigate disruptions to safeguard the civilian population. This is the portion where Taddeo will agree. Since she mentions that the Just War theory should be applied to cyberwarfare, should agree that nations need to develop robust measures and recovery strategies. Furthermore, the last sentence in the last paragraph of the article states the international collaboration and information sharing is a crucial factor in combating against hybrid warfare. Taddeo will agree with this statement.

Through the lens of deontology, it will argue that deliberately conducting cyber-attacks on critical infrastructures, and non-military infrastructures which have a negative impact on civilians is not right, since the intentions behind it are not moral. Also, these types of cyber-attacks demonstrate that people behind them do not respect other people. However, in this second case, having a strategy to develop robust security measures to assist mitigating harm done to civilians has rightful intentions. I think that deontology will be in support of this viewpoint, since the intentions behind it are one that respects people and wants to protect them. Plus, deontology mentions people have a duty to do the right thing. In this case, the people who conduct offensive cyber operations have a duty to conduct them in a way that does not involve the harm of a civilian. Also, those people who work on defensive security, critical infrastructures, have a duty develop security measures to defend civilians from cyber-attacks.

Conclusion

Overall, the introduction of cybersecurity has brought a new realm in warfare. Instead of just conventional means cybersecurity has introduced hybrid warfare. Now nations conduct cyber operations that attack critical infrastructures, supply chains, etc. These attacks can cripple a country's national security, economy, and potentially the health of civilians. The actions that were described in the article are not part of a just war. The Just War Theory follows a principle that attacks should not be conducted on non-combatants and minimize harm to them. The article described how cyberwarfare can impact civilians, and using deontology, and both Boylan's and Taddeo's concept they show that cyberwarfare has created grey spots in warfare that are difficult to determine what is right or wrong.

Though Taddeo and Boylan have made good points, there are flaws. I agree that wars should be conducted for rightful reasons, but perhaps some of the cyber attacks conducted in cyber operations are done for the right reason. For example, if a nation was constructing nuclear weapons, that is potential harm to people, the use of non-conventional tactics can prevent that threat from forming. Also, in terms of Taddeo's concept, it will be very difficult to have different nations agree on how to rightfully conduct cyberwarfare, since there are different opinions on what is considered right or wrong. Deontology shares some flaws. The same way that deontology argues that the actions described in the article were not part of a just war, the same could be said that deontology agrees the actions were part of a just war. In that case, it would be subjective on what actions are considered a part of Just War.