**Introduction**

The article *Digital Battlegrounds: Evolving Hybrid Kinetic Warfare* discusses hybrid warfare during the Israel- Hamas war in October 2023. The coordinated cyber warfare attacks were facilitated by four hacktivist groups: Cyber Av3ngers, Anonymous Sudan, AnonGhost, and Killnet. The first attack occurred on the evening of October 6 when a pro-Iranian hacktivists group called Cyber Av3ngers launched a Distributed Denial of Service (DDoS) attack against the electric industry in Israel. The second attack occurred in the early morning of October 7 when hacktivists groups called Anonymous Sudan and AnonGhost launched a DDoS attack on Israel’s warning system called “Red Color.” This attack caused a disruption in the communication system in Israel. The hacktivists group called Killnet admitted to the DDoS attack on the Israeli government and Discount Bank Israel websites. These hybrid warfare tactics include non-kinetic tactics, such as cyberattacks on critical infrastructure, information warfare, and disruptions to communications. In their articles, some concepts mentioned by Michael Boylan and Mariarosaria Taddedo will help explain my analysis of this case. In this Case Analysis, I will argue that the virtue of ethics shows us that these actions could not be part of a just war because these actions do not align with the rules of just war.

**Michael Boylan: “Can There Be a Just Cyber War?”**

Michael Boylan’s piece *Can There Be a Just Cyber War?* covered some concepts that will help us agree that the actions taken during the Israel-Hamas war could not be part of a just war. One of the concepts Boylan discussed was “jus ad bellum and just in bello.” The cyberwarfare attacks during the Israel-Hamas war do not align with jus ad bellum and jus in bello. Jus ad bellum focuses on the why of the war, in which force is considered just, legitimate, has right intention, and last resort. Jus in bello focuses on the right conduct in war, in which the use of force must be proportionate, with no discrimination, and necessary. The attacks facilitated by the hacktivists during the Israel-Hamas war focused on the opposite principles of jus ad bellum and jus in bello. Each hacktivists group conducted a cyberwarfare that was not authorized legally, the target (Israel) was not aware of, which is a sabotage, the intention was wrong especially when they targeted the communication infrastructure, it was discriminatory towards the Jews, and it was not the last resort for them to attack Israel. Virtue ethics suggests that individuals involved in cyberwarfare should have virtues that emphasize the importance of ethical decision-making and actions promoting the beneficial use of cyber capabilities. The hacktivists groups mentioned earlier lack virtues such as justice and use cyber capabilities for the wrong purposes.

Another concept discussed by Boylan was “belligerent kraterists.” Boylan said, “Rules thus constrain war confound the belligerent kraterist. Belligerent kraterists obey only the rules of self-interest – hardly a moral rule.” Belligerent kraterists believe the ultimate measure of right and wrong is success. The attackers believed their actions were justified because they facilitated attacks on Israel that were successful regardless of ethical implications. Virtues of ethics say that cyberwarriors should seek wisdom and prudence in their decision-making, considering the consequences of their actions. The groups of attackers did not consider the consequences of their actions, only their self-interests.

Boylan also discussed the concept of “arete soldiers,” which arete means virtue or excellence. Arete is relevant to soldiers and virtue ethics, emphasizing enabling people to do their full potential and live flourishing lives. In this case, the attackers were the soldiers of their own. They succeed in their attacks. They were excellent in their duty; however, their actions did not contribute to a flourishing life. Their cyberwarfare caused chaos, which doesn’t align with virtue ethics. The attackers’ virtue of courage to execute the attack on Israel was not moral.

Another concept introduced by Boylan was the “fifth column person.” In this case, hacktivist groups were the fifth column because they undermined Israel in favor of Hamas during the Israel-Hamas war. The actions of the groups of hacktivists were more of sabotage than an act of war and, therefore, cannot be considered just war. Sabotage as a vice, involves causing harm and damage to others and undermines the common good, which is the opposite of the principle of virtue ethics. Just war does not include the fifth column person. The actions of the fifth column person go against the principles of just war.

**Mariarosaria Taddedo, “An Analysis for a Just Cyber Warfare,”4th International Conference on Cyber Conflict, 2012**

Mariarosaria Taddedo wrote an article called *An Analysis for a Just Cyber Warfare.* She talked about some concepts necessary in this case analysis to prove why the actions of the hacktivist groups were not just war and did not align with the virtue of ethics. One of the concepts she discussed was “necessary but not sufficient.” The actions of the groups of hacktivists fall under cyber warfare, also known as hybrid warfare. In this case, traditional warfare is necessary for cyberwarfare actions, but it’s insufficient because sabotage or espionage exists. Cyber warfare is necessary and sufficient for traditional warfare. It does not sound appealing that cyber warfare is necessary for traditional warfare because cyberwarfare can cause more harm than traditional warfare. Taddedo illustrated the difference between traditional and cyber warfare and what they cover. Traditional warfare’s harm is violent and physical, includes civilians, and is done by humans. Cyber warfare harms both violent and non-violent, both physical and non-physical, civilians and military, and humans and artificial. Traditional war can employ hackers to help them with their goals, such as virtually attacking an enemy while avoiding bloodshed. This instance will agree with the virtue ethics of preventing violence. Cyber warfare conducted by hacktivists cannot employ traditional warfare because it would defeat their purpose of being black hat hackers, and it would be doing things ethically.

Another concept Taddedo discussed was “transversality.” The actions facilitated by the groups of hacktivists when they facilitated different DDoS attacks on Israel did not directly kill any civilians. However, the result of their actions caused bloodshed and harm towards the civilians. This action is transversality where all the attackers’ successful attacks somehow connected and collaborated in taking down Israel, which goes against the rule of just war. The attack had a tangible effect on many civilians and caused a number of casualties.

Taddedo also discussed “discrimination and non-combatant immunity.” The discrimination and non-combatant immunity principle prevents harm to innocent people. In a just war, the military armed forces are able to direct the attack to a target like a government building. In cyber warfare, the attack can affect civilians. For instance, deleting records that may contain vital information of the citizens is physically harmless, but it still affects innocent people. Another instance is cyber warfare to disclose classified information that contains innocent civilians' information. Cyber warfare reduces bloodshed but is not able to abide by the principle of “discrimination and non-combatant immunity” and, therefore, cannot be part of just war.

Another concept discussed by Taddedo is “information ethics.” She stated, “An entity loses its rights to exist and flourish when it conflicts with the rights of other entities or with the well-being of the infosphere.” When Anonymous Sudan attacked the Red Color system in Israel, they interrupted the rights of Israel to be aware of incoming war. The Israelis could not secure themselves because the warning system was compromised. The group of hacktivists loses their right to exist. The action does not comply with the rules of just war. The attack does not align with virtue ethics because the attack caused chaos, not the greater good.

**Conclusion**

I think I have used the concepts necessary to explain my case analysis. Hacking, cyber warfare, or hybrid warfare is considered an unethical act, so it cannot be considered a just war. Just war says war must be for a just cause, lawfully declared by lawful authority, the intention behind it must be good, and other ways of resolving the problem should have been tried first. The rules of just war agree with the core principles of virtue ethics, which promote flourishing and a good life, both for the individual and society. All the attacks that targeted Israel are considered terrorist acts. Anything considered terrorist cannot be just war. Israel had a dome that protected its people from any harm, but it was compromised. Their communication system was also compromised. Just war involves both parties to be aware of that battle. It was a surprise attack on Israel. I think that virtue ethics explained well how the attacks were not considered ethical.