Case Analysis: Cyberwar - Fair Fight or Digital Fallout?

Introduction.

The rules of war have fundamentally changed with cyber warfare. It is no longer just about tanks, soldiers, or bombs. It can begin with just a few lines of code. Paul Veeneman's article *Digital Battlegrounds: Evolving Hybrid Kinetic Warfare* is a great example of how cyber operations can be used alongside traditional military operations. Rather than one form of action replacing another, we are seeing a hybrid form of actions directly blended with traditional military operations. While the method of cyberattacks may not leave physical buildings in ruins or take human life directly, they can disrupt a power grid, affect lines of communication, and even intrude or influence the decision-making of a nation-state. The civilian-military line is blurred when it comes to cyberattacks, and this is where ethical issues arose. Michael Boylan introduces Just war Theory and questions whether cyber actions, even the "clean" or bloodless forms can be truly just. Mariarosario Taddeo elaborates even further with her thoughts that we cannot adhere strictly to traditional rules of war any longer. She introduces the idea of thinking about the entire digital place known as the "infosphere" and considering harm differently–not only from a perspective of physical destruction. This is where contractarianism fits in. It relates to fairness and whether people would agree to certain actions if they did not know what side they would be on. In this analysis, I will argue that contractarianism illustrates that these cyber actions could not be part of a just war, because they break the kind of fair rules no one would honestly agree to if they were thinking about everyone–not just their own side.

Analyzing Using Boylan's Perspective.

Michael Boylan addresses significant concerns related to cyberwar and justice. He bases his argument on Just War Theory, which states that war is only just if there are conditions that are

met such as: there must be a real reason to fight, it must be of last resort, and it must avoid harming civilians. It becomes extremely complicated to determine these criteria when it comes to cyberwar. There may not be bombs or blood, but the rationale for violence and harm may remain similar, if not more excessive.

Central to Boylan's argument is the idea of "positive good." Moral action is not simply to not do harm, rather, one must demonstrate that the act they are taking is morally meaningful and beneficial. So, if a state decides to launch a cyberattack, the best scenario would be that the objective of the state is not to win, but rather to stop real harm, and restore some positive good. The problem lies in the reality that much of what we consider cyberattacks do not fit that mold.

The accounts taken from Veeneman's article, for example, clearly illustrate cyberattacks being used to weaken enemy systems, jam communication networks, or to facilitate a physical attack. There are usually no public notices to those who may be affected at the point of impact, which in many cases raises the general level of insecurity and uncertainty. In fact, the lines between military and civilian targets are not clearly defined. Power grids, banks, and hospitals are all at risk of these cyberattacks and are considered collateral damage. From Boylan's viewpoint, cyberattacks do not fit the criteria of "positive good" because they are not defensive actions to prevent harm to individuals, rather power is simply leveraged to create an offensive weapon to use over enemy interests.

Now let's think about this through the lens of contractarianism. This approach says that we should only accept rules that everyone would agree to–especially if they did not know their role ahead of time. Picture yourself behind a "veil of ignorance," with no clue if you will end up a soldier, a civilian, or someone caught in the middle. Would you agree that someone can

deactivate your energy, or wipe your data in an instant without notice? Most people would not, as that would be too risky and unfair.

This definitely relates to another of Boylan's concerns: proportionality. According to him, any military action must be proportionate. One cannot use excessive force simply because they possess the means. For example, a cyberattack that results in a city-wide blackout, or knocks out emergency systems, does not necessarily kill anyone outright, but it is still a threat to life. Disrupting a city can happen quickly with cyberwar. If one is following the tenets of fairness–as contractarianism asks–then the chances are that they are not going to accept that level of threat or injustice, unless they absolutely have to.

Accountability is another concern. In a traditional conflict, the blame for an attack can be assigned to a direct individual or group. However, cyberwar is typically anonymous. This makes it almost impossible to hold someone to account and seek justice afterward. Contractarianism requires a fair social contract, but this does not work under bad faith when breaches such cyber occurrences have no repercussions for bad actors. If no one can be held responsible, then in essence the agreement falls apart, which leads to disastrous consequences.

Boylan also addresses the concern of noncombatant immunity. Just war theory states that civilians should be excluded from direct military engagement. However, cyberwar makes this distinction blurrier. Civilians may use the same digital infrastructure as the military, which places them in a deadly choke point. Thus, deactivating a communication system, for example, means that civilians and military personnel are both subject to the fallout. This breaches both Boylan's ethical consideration and the fairness idea in contractarianism, since no one would agree to be part of a system where they could become a casualty without even being involved.

Ultimately, both Boylan's viewpoint and the contractarianism ethics converge on the same conclusion. These cyber actions–no matter how strategic they might be–fail the fairness test; they risk harm to people who did not choose to be involved, and they do not provide moral good in return. Therefore, while the broader war might be just, this does not make cyber actions just.

Analyzing Using Taddeo's Perspective.

Mariarosario Taddeo takes a different route than Boylan and agrees that Just War Theory still applies; however, she says that it is not enough for cyberwar. The reason is that the rules involved in traditional war are typically based on notions of violence, bloodshed, and physical destruction. In contrast, cyberwar may not appear to be that way. It is quieter, sneakier, and often goes unnoticed. So, continuing to use old rules does not capture what is actually happening. Taddeo introduces the ethical approach termed Information Ethics, that is concerned with how a cyber action would affect the entire digital environment–which she calls the "Infosphere." The infosphere includes people, data, networks, and everything digital. The idea is that harm does not need to be physical to be serious. Therefore, harming a hospital's computer system or tampering with emergency response networks causes serious harm even if no one sees it happen.

One distinguishing feature Taddeo talks about is "transversality." The actions involved in cyberwar span a multitude of lines at once. They can be violent or non-violent, involve soldiers or civilians, and take place in both physical and non-physical spaces. That makes it hard to define what counts as a legitimate target or who is even participating. Someone may commit a cyberattack while sitting at home and never make physical contact with a weapon; that blurs the line between combatants and non-combatants. In her view, as a result, we need a new way to judge cyber actions. She elaborates three core ethical principles for a just cyberwar. First,

cyberwar should only target entities that cause real harm to the infosphere. Second, the goal should be to stop that harm, not to gain power or control. Third, cyberwar should never be used just to make the system better.

When those principles are examined and compared to the actions discussed in Veeneman's article, it becomes obvious that there is an issue. They are used to gaining an advantage before a physical conflict begins. However, they often do not fulfill the requirement of stopping a harmful threat. Sometimes, they create harm themselves; they can shut down communications, confuse civilians, or target digital resources, for example. All of which may achieve a military objective but create turmoil for the civilian population.

Taddeo's second principle states that a war should only be reactive–not a way to improve or reshape things. Rather, many cyber actions are specifically designed to do exactly the opposite: they are intended to change the battlefield or weaken a system before it becomes a significant threat. This is not defending oneself against threat–it is manipulating tactics that violate the rule.

Putting this into contractarian terms helps clear things up. Behind the "veil of ignorance," you would never consent to a rule that allows people to interfere with your digital life with no notice or without any means to defend yourself. You might be a civilian relying on electricity, medical records, or access to emergency alerts; if those systems get hit in a cyberattack, you are in danger. A fair contract would account for a person in your situation–not leave them exposed.

Contractarianism also says that any rule should be the one that one would accept even if they ended up being the worst off. In cyberwar, the worst off are often civilian populations who have absolutely no clue or say in what is going on. Even if they are not directly part of the combat, their lives are affected, and no one would agree to rules that allow that kind of risk,

especially when there is no way to fight back or prepare for it. Taddeo's ethics match this idea. Her focus on the infosphere includes everyone, not just military targets, which aligns with the contractarianism view that posits that everyone's interest should count equally.

So, even though cyberwar might look less violent, it still causes serious harm–not only that, it also often creates harm in an unfair, and unpredictable way. Taddeo's analysis, supported by contractarianism, shows that many of cyber actions are not just; they do not meet fair standards, and they risk hurting people who never chose to be involved.

Conclusion.

After considering everything, it is evident that the cyber actions detailed in Veeneman's article just do not pass the ethical test. Both Boylan and Taddeo illustrate how cyberwar poses severe challenges for traditional notions of justice. Boylan leans into Just War Theory and points out how these actions fail to protect civilians, achieve genuine goodness, or keep things proportional. Taddeo digs into how cyberwar messes with the boundaries of war altogether and raises the fact that we need a better way to measure harm, from the perspective of Information Ethics. Combining those ideas with contractarianism, it becomes even more obvious–these actions are not something anyone would agree to if they did not know their role in the conflict. Some people may argue that cyberwar is better than conventional war because it can minimize bloodshed and destruction to physical systems. That is a valid point. But ultimately, harm is more than broken bones or demolished buildings. Disrupting someone's life digitally can be just as damaging. Plus, it is much easier to cause collateral damage when civilians are connected to the same system as the military. There is no perfect solution here. Cyberwars just complicate everything. Still, if we are aiming for decisions that feel fair to everyone–regardless of which

side they are on–we have got to stick to rules that protect people from harm they never signed up for. It is not easy, but that is something worth careful consideration.

This paper is my own work, and I have proofread it,

Daniel Akpovi.