Introduction

Cyber Warfare has become really common in modern day conflict. Instead of actually people fighting with tanks and troops, there are now digital attacks that can take down hospitals, power grids, or even just flood the internet with false information. This type of thing can happen from far away and ruin people's everyday lives. Cyber attacks are mostly targeted towards civilians by taking away their essential services and starting internal conflict within the country. Some methods of cyber attacks are Ddosing which is attacks on government websites, malicious softwares to shut things down, and false information to spread. These actions don't sound as deadly to actual war, but they impact the world a lot, you could possibly lose someone which isn't a minor problem. In this case analysis, I will be using the Kantian deontology tool that goes against these types of tactics because they go against the moral rules by treating people like tools to gain something, rather than respecting them. Using the framework of Boylan and Taddeo I will also be showing how they crossed the ethical rules even if war could be justified.

Boylan Concepts

James Boylan's ethical approach to this is that morality is more than just about getting good results, instead it is about doing the right thing because it is the right thing to do. By noticing his clear principles you can see the comparison with Kant's morals, especially from the idea that we should act on only on principles that we would want everyone else to follow as well. If we use these principles for cyberwarfare, some things wouldn't pass. For example using malware to shut down a hospital system even if it would damage your enemies, imagine if every country started doing that then war would be even worse and nobody would be safe. Another important thing from Kant and Boylan is that you shouldn't use people as tools to get something. Yet that is what happens when it comes to cyberattacks. Misinformation, for example, is designed to manipulate how people think and feel about certain situations. When people are told lies and propaganda it is meant to influence the public opinion which leads to fear or them being confused. This type of action violates the dignity of the people since you are dragging them into a situation that they are not in and using them as tools to go against themselves. This type of manipulation would not be justified under the Kantian perspective.

Boylan is really big on the importance of consistency. A government that claims to value human rights, but they are undermining civilian well being through cyberattacks isn't consistent at all. If you claim that you value human rights and freedom, you must show that even during conflict, this means you have to apply your morals to everything you do regardless of anything. Cyberattacks go against these principles and are a double standard, since they only message the civilian when it is convenient for them, not when

they interfere with the military. Boylan also states that ethical behavior means you must be transparent and accountable, when it comes to cyberwarfare you don't really know who is attacking you and this lack of accountability interferes with Kantian ethics. Another example is how cyberwarfare might take us away from actual violence, but it actually causes damage. Because cyberattacks can be done without any physical or direct contact, it may seem like they aren't as harmful. But the effects such as turning off power or shutting down hospitals can cause life threatening situations, just because it isn't someone killing doesn't make it any better. If an action disrespects human life or their dignity, then it is unethical regardless of whether it involves traditional violence. Looking at cyberwarfare through Boylan perspective it shows that many tactics fail the ethical test, they violate the principle of treating everyone with respect. The right approach even if there is a war going on, is to limit cyberattacks to strictly the military instead of the civilians. Just because they are digital attacks does not mean you can just break the moral codes, instead you should be even more careful. Just because this is somewhat a new way to attack someone doesn't mean we have new values.

Taddeo Concepts

Mariarosaria Taddeo looks at how cyberwarfare fits and doesn't fit into the traditional things that make war what it is. She states that cyberattacks are different from regular warfare in many ways, for example they are anonymous, untraceable, and don't all the time involve physical damage. But that doesn't mean they aren't harmless, Taddeo argues that we still need strong ethical rules to try and control these digital actions. One of her key concerns is that you shouldn't involve civilians with what is going on with the military which is called the principle of discrimination, when cyberattacks hit hospitals or schools they are breaking this rule. Even if the goal of the attack is to damage the enemy the people who suffer the most are the people that had nothing to do with the conflict. Taddeo also speaks about the amount of harm that the military caused should be balanced by the benefits that could come with it. A cyberattack that shutdowns medical services or spreads misinformation costs more harm than any short term military gain. For example, if a virus were to spread again and there was a cyberattack that spread misinformation that could confuse people about what to do then it could lead to death. That type of damage isn't worth the risk for cyberattacks. Another issue she has is people are barely accountable for their actions. A problem with cyberwarfare is that it is hard to know who is behind an attack. Skilled hackers could easily hide their identities or use VPNs, if nobody is responsible for these attacks it makes it harder to enforce moral rules.

Taddeo also highlights how cyberwarfare makes it harder to keep up with out ethical norms. Since these attacks happen in mostly legal or gray areas, they can stretch the rules to make it look morally right. Cyber operations usually involve deceptive

strategies, including misinformation and propaganda. These strategies attack the integrity of public discourse, which makes it harder for democratic societies to function. She also states that cyberwarfare can make a conflict last longer rather than containing it, cyberattacks can start problems between other countries that aren't even involved in war. Another concern is the loss of control, as countries are relying on algorithms and systems they are risking the chance of creating tools that don't listen to human judgment. She warns that relying on these systems removes humans from the equation, which reduces accountability and gives them room for more unjustified actions.

From Taddeo's perspective, ethical cyberwarfare must have clear rules, transparency, and protecting civilians that aren't involved. Her view on cyberwarfare aligns with Kantian ethics, which prioritize respect for people and being rational. Cyberattacks that violate these principles go against the moral foundations of which his theory is built on. So, even if a war is okay to have, using cyberattacks that target people or cause damage is not. Taddeo reminds us that just because it is digital does not mean it does not have to follow the moral rules. If anything, since the internet is advancing it requires even more care. Just because it is a new thing doesn't mean it gets a free pass, ethics still apply to it.

Conclusion

After looking at both perspectives of Boylan and Taddeo, it is clear that cyber warfare tactics such as disabling hospitals and spreading misinformation doesn't pass the test of ethical behavior. They violate the key principles of treating people with dignity and being consistent in your moral beliefs. Some might argue that cyberwarfare is a way to end traditional violence, but Kantian ethics doesn't really focus on the end results, it cares about our actions more. If we were to put our morals aside for efficiency then it could become a trend to do so which could lead to being morally inconsistent. In the end, the digital world doesn't excuse our unethical behavior, you just need to be more careful. Boylan and Taddeo both had great points on why we need to stick to our ethical commitments, even in cyberwarfare. Which means protecting people, respecting each other, and acting with integrity, no matter the situation. If we stop doing that the world is gonna take a turn for the worse.