Ethics of Just Cyberwar Through Contractarian Reasoning

Veeneman details a few examples of cyberwarfare being carried out in the recent Israel-Hamas conflict. One of these examples is one where Anonymous Sudan and AnonGhost worked together to interfere with the Israeli communications system. They took ahold of the Red Alert system, leading to numerous false alarms and scrambling communications in the early hours of October 7th. This resulted in increased panic and confusion when Hamas would physically attack. Additionally, this kind of cyber act may not be constrained to the boundaries of war. Veeneman discusses how the impacts can linger even into the postwar recovery, hindering the nation's ability to recover and leaving malware behind that can strike at any time in the future, triggering war and chaos once more. This then brings up the moral dilemma of if these actions fall under just war. On the one side, hampering enemy communications has always been a tactic of war. On the other, these impacts typically do not last long after the war ends. Due to the lingering impacts of malware, it can be argued that under contractarianism that certain cyberwarfare tactics are immoral.

Boylan discusses that there are two aspects to justifying warfare. The first is *ad bellum*, which is the justification for going to war. This aspect covers what would be a justified or unjustified reason for going to war and instigating war. Under this, a nation that is attacked by another would have just cause for going to war. However, a nation that argues that another nation is a historical threat to themselves and attacks that nation accordingly is likely unjustified. The second concept discussed is that of *in bello*, or actions that occur during wartime. This is much more contested, especially in the context of modern warfare. Many *in bello* actions that are or are not permissible are covered under the Geneva Convention. However, as discussed by Boylan, the Geneva Convention has not been updated since 1949 and as such has no provisions for the limits

of cyberwar. What is covered is that militaries are not to directly target civilians and that there are certain limits for the destruction of infrastructure.

Under this understanding, one must first establish that the war itself is just in order for an initial cybersecurity act to be just. In the example above, with Hamas as the initial attacking party and presumed aggressor, it can be argued that its actions were likely unjust. However, if Ukraine were to conduct a cyberattack against Russia in the wake of its invasion, it likely would be viewed as justified. In the example with Hamas, any further cyberattacks would fall under an unjust *in bello* act as they are the established aggressor party. However, if Ukraine were to conduct further cyberattacks, they would have justified *in bello* as the defensive party. However, Ukraine in this hypothetical must also act as a responsible party to continue having justified actions under *in bello*, even as the defensive party. The regular acts of war that are forbidden still apply even if they are conducted through cyber means. They cannot starve the populace of Russia using a cyberattack to completely block off their logistics system. They cannot use a cyberattack to shut down civilian hospitals. However, they can use a cyberattack to disrupt military communications.

Where the line becomes messy is the lingering effects of cyberattack as discussed by Veeneman. A cleaner line can be drawn by looking to contractarianism. Under contractarianism, morality is defined by the rules that we all agree to as members of a society. While this is often applied within the context of a singular society or nation-state, there is precedence for this being applied internationally through the Geneva Conventions. Many of the social contracts under contractarianism are unspoken and implicit, an idea which can be used when arguing for extending the explicit and agreed upon international contracts that have already been drawn. The Geneva Conventions detail that certain lasting harms cannot be applied to nations, even during

otherwise just wars. Another nation cannot make agricultural land unusable, it cannot fully destroy infrastructure that is key to life, etc. As such, one can conclude that leaving malware behind in the postwar era that can be triggered and cause catastrophic effects violates this contract between nations. Additionally, there is precedent that the only agreement for access to territory, resources, and people within a nation in a postwar era must be outlined by the treaties signed. Persisting malware violates this as it provides unknown and unrestrained access to a nation's interior that is not granted during treaty negotiations. Considering this, a cyberattack can be just under contractarianism, but it must follow the logical lines of contracts already established.

Taddeo proposes the counterargument that the just war theory used by Boylan in their argument is not comprehensive enough to truly evaluate cyberwarfare. They argue using the principle of war as last resort to state the idea that nations will be forced to pick unethical actions no matter what they do. If they choose to conduct a cyberattack, that will be viewed as an act of war under the just war theory, even if no blood is shed. But if they do not conduct a cyberattack and that leads to a bloody war, then they have also committed an unethical act under the current framework. Additionally, they argue that the lines between combatant and civilian have become too blurred in the age of cyberwar for traditional models of war theory and ethics to apply. Those acting as civilians can now carry out cyberattacks from their home, thereby making them hidden combatants. The author posits the concern that this will lead to either heavy surveillance and privacy rights violations or will lead to indiscriminate killings as anyone could be a potential combatant.

Placing Taddeo's argument in the context of Veeneman's article, it becomes evident that there is some merit. In the context of cyberattack against communication networks, there is

evidence that these attacks do not stay in the realm of targeting military communications. Instead, these lead to civilian communications being impacted. Additionally, this impact towards communications across the board can cause more panic and death as civilians may not be properly warned and evacuated from active warzones. In an era where these warzones can move very quickly, it is crucial that communications for civilians remain unimpacted. Further, the concern of privacy violations can potentially already be seen. There have been multiple nations using multiple methods in the past few years to crack down on internet anonymity, from Russia restricting what can be displayed on the internet and by who to the UK implementing age verification laws that do nothing but collect ID data. Many of these acts are partially or fully under the guise of preventing terrorist attacks. On the other side, it can also be seen how the blurring of the lines between civilian and combatant can result in utter disaster. In the current Israel-Hamas war, there is not even any current accurate accounts of civilian deaths because it cannot be agreed by both sides who *acts* as a civilian and who *is* a civilian.

Through Taddeo's argument, under the contractarian model there is no remedy. Under contractarianism, we agree to follow implicit rules. But there are no true rules for conducting oneself in cyberspace, let alone what the procedures are for cyberwarfare. Some nations take more cautious approaches and refrain, others commit fully to acts that cripple their enemies. Through this, it can be seen as a complete failing under contractarianism altogether to be unable to formulate a social contract. The age of cyberwarfare presents the worst case scenario that the original theorizes of contractarianism feared: anarchy. Until a contract is agreed upon generally by nations for cyberwarfare, any act of cyberwar will continue to be a moral failure under contractarianism.

Cyberwarfare is a difficult topic to discuss and even more difficult to put into the context of a moral framework. However, I believe that viewing this issue through contractarianism, that acts of cyberwar in many instances are moral failings. But, these moral failings must be put into the context of the other options available to nations, of which there often are no good options. War in general is complex and the morals of it have been argued over for centuries and will continue to be argued over. To many scholars, any act of war will always be a moral failing, yet it seems there will never be an end to war. So knowing this and the bloodier options that are on the table, cyberwarfare, while being a moral failing itself, is not as severe a moral failing. If an immoral act must occur, then it should be the least immoral act of the choices available.