Case analysis on Cyberwar

by

Alan Schneider

In online articles covered by NBC news and MEMO. The authors discuss the ongoing and troubling escalation of cyberattacks between Iran and Israel. Specific details of the escalation beginning with an Iranian attributed attack of Israeli water and sanitation facilities. Israels response, against computer facilities at Iran's largest port, then unattributed attacks targeting Iranian Railways computer systems. Culminating in Iranian cyberattacks against Hillel Yaffe Hospital in Hadera and the responding unattributed attacks against Iranian gas stations. This raises international concerns that as attacks become more sophisticated and focused on critical infrastructure, fatalities will be an inevitable result of this tit- for-tat cycle between these two nations. In this Case Analysis I will argue that deontology shows us that the cyberwar between Israel and Iran can be just if both sides follow principles of just cause, proportionality and target discrimination.

To understand what constitutes a just war and how one could be waged between these two nations, we turn to Michael Bolan’s insights into how cyberwar fits into traditional ideas of a just war. Under the traditional concept of war, it is an aggressive act by one state against the territory or sovereignty of another state. Whether for territorial expansion, resource exploitation or in service to national strategic or tactical goals. It is ostensibly regulated by internationally recognized rules and constraints labeled jus ad bellum and constraints that comprise whether a war is just called jus in bello. Both frame the actions of the attacking state as immoral because the attacking state caused the conflict. This idea of an immoral act features prominently in the Jus ad bellum principle of just cause; that it is just to conduct war in your nations defense or to achieve humanitarian intervention. One need look no further than the Russian invasion of Ukraine to see an example of just cause in action. Particularly when considering Russian war crimes against civilians in places like Bucha or forced deportation of Ukrainian civilians in Mariupol. With that in mind Boylan frames three issues with using traditional justifications for war when it relates to cyberwarfare.

First is the idea of territoriality, while attack or invasion of a nations territory or sovereignty has historically been part and parcel to the idea of an aggressive act, precipitating a just cause of war. Cyberwarfare doesn’t involve troops crossing borders or seizing sovereign land and resources. There are no recognized borders defining the internet and no resources to be seized per se. The second issue is greater problems with attribution. Traditionally, attribution is easily answered when there are physical events of individuals crossing territorial lines and occupying land and strategic positions in an opposing country. Cyberwarfare on the other hand enjoys an almost built in anonymity when conducting aggressive acts. Not only does the distributed nature of the internet and patchwork governance hamper efforts to link offender to offense. It is further complicated by state sponsored proxies given the tools to conduct effective cyberoperations in accordance with their patrons’ goals, but not in their name. The third that relates to attribution is proper target distinction. Target distinction is a critical part of just war theory. In jus in bello rules, warring factions may attack military targets or civilian/non-combatant targets that are enabling the military to fulfill its mission. But this becomes a problem when dealing with modern dual use infrastructure and conducting cyberwarfare. An example would be if an electrical grid supplying a military base was a target, but it supplies not only the military but hospital and water distribution as well. Then an attack on the electric grid to harm the military might have considerable collateral damage on hospitals and water treatment with the resultant loss of non-combatant human life, which can potentially violate Jus in bello principles of proportionality and necessity.

So, if we use Boylan's conceptualization of the ethical roadblocks faced when conducting cyber war against a backdrop of traditional theories of war, can a cyberwar be just between Israel and Iran? The idea of proportionality and target distinction takes center stage in this discussion. The Iranian attack on Israeli water supplies in which hackers attempted to alter water chlorine levels to dangerously high levels before being detected and stopped was not proportional or distinct in its targeting. The water treatment facilities affected could not be reliably tied to any military use. And if they had been successful, could have caused unnecessary suffering and death of civilians. The same lack of proportionality and target distinction is in evidence during with the Hillel Yaffe Hospital cyberattack. Again, proportionality and target discrimination are an issue, as Hillel Yaffe is a civilian hospital that cannot reliably be said to support the military or be a legitimate military target. In contrast, Israels cyberattacks are proportional in nature. No water treatment or hospitals were attacked. But they do fail the jus in bello test in terms of target distinction. Neither the port, railway, or gas systems can be reliably tied to military support or objective. A just cyberwar is possible, if one side or another takes extra step to ensure cyber responses are proportional, clearly distinguishes between military and civilian targets and intentionally only attacks military objectives.

Deontology teaches that the actions one takes in any given situation is the action that is based on the best reasons according to shared rules. An ethical 'line in the sand' that prevents us from acting in certain ways either toward other people or toward ourselves. Actions that align with these rules are ethical, while actions that don't aren't. If we apply deontological ethics to the Iranian/Israeli cyberconflict, the choices are clear. Firm adherence to just war principles of just cause, proportionality and target discrimination must be applied. First, Iran or Israel must have a just cause to conduct cyber-attacks on each other. Israels alleged assassination of an Iranian nuclear scientist which prompted the rise in cyberattacks can be considered an aggressive act that meets the just cause requirement. However, Iran's attacks against Saudi Arabian oil fields, harassment of civilian and military vessels in international waters, as well as the kidnapping and detainment of not only US but British military personnel without cause could also be considered just cause for multiple nations to attack Iran. Second, critical civilian infrastructure like water treatment, hospitals, and petroleum distribution, must be off the table in terms of disruption and attack. If dual use is at issue, then clear steps must be taken to ensure the damage is confined as much as is possible to the military objective and limit damage causing unnecessary non-combatant suffering. In the end firm adherence to those principles follows deontological ethics to do right within the confines of accepted norms and rules, even when others do not.

Next, we look at Mariarosaria Taddeo insights into the transversality and insufficiency of Just war theory when applied to cyberwarfare. Traditional war is the use of a state's violence through their military forces to determine the conditions of governance over a determined territory. This type of state violence invariably leads to loss of human life and the damage of both military and civilian infrastructures. Traditional rules of warfare are centered around goals of reducing damage to civilian infrastructure thereby minimizing non-combatant suffering while pursuing military objectives to overpower the enemy. This is where cyber warfare differs from its traditional counterpart. Cyber-attacks may involve malware to disrupt or deny access to critical military infrastructure causing severe damage to the enemy without exerting physical force or violence. It also does not directly involve human beings in committing the attack. But, while cyber-warfare ostensibly causes damage in a non-physical or violent way, it can be just as dangerous as traditional warfare. This is where Taddeo introduces the concept of transversality in cyberwarfare. This transversality cuts across any traditional warfare distinction such as 'violent-non-violent', 'civil-military', 'human agents-artificial agents'. An aspect that is at odds with traditional distinctions of warfare, which is violent, conducted by militaries and mainly by human agents. Essentially transversality, as it applies to cyber-warfare is blurring of lines between levels of violence and escalation from non-violent to more violent forms. A simple example could be the cyber-attack on a radar facility that is designed to allow aircraft to penetrate that countries air defenses to strike a legitimated military target. But also results in a civilian air disaster due to its dual military/civilian use. A non-violent intent with a violent result.

With this idea of transversality in mind, Taddeo begins to address the three inadequacies of just war theory: last resort, more good than harm and non-combatant immunity when applied to cyber-warfare. First is the just war principle of last resort. This principle centers around the idea that a state may only resort to war if it has exhausted all reasonable alternatives to resolve the conflict in question. That war, by the very nature of its propensity for violence and suffering should be avoided, unless it is the only reasonable way for a state to defend itself. When taking cyberwarfare into account this principle becomes less immediate, as a cyber war maybe bloodless and not involve physical violence, influencing states to consider this form of war to resolve tensions and avert a potential traditional war. Using cyberwarfare as a first rather than last resort that is in essence breaching the principle of war as last resort and committing an unethical first strike and an unprovoked act of war. Second is the just war principle of 'more good than harm'. A state must balance universal goods expected from the decision to wage war against the universal evils that will result. A state is only justified if the goods are proportional to evils. In traditional warfare the cost is readily assessed in terms of casualties and physical damage. In cyberwarfare however this balance becomes more problematic, as attacks are likely to cause very few casualties and unlikely to cause physical destruction. Thereby all non-violent cases of cyberwarfare could potentially comply with this principle. For example, destroying a database of important historical records, the action would be unethical but still comply with the principle as it does not rise to the level of physical damage. The last inadequacy Taddeo addresses is similar in form to the problem Boylan discusses. That of the principles of discrimination and 'non-combatant immunity'. Traditional warfare provides distinction between military civilian in an effort to reduce bloodshed and violence against non-combatants. Conducting cyberwarfare blurs the line between combatants and non-combatants, where wearing a uniform is no longer a sufficient to identify someone's status. Civilians of various governments routinely take part in defensive and offensive cyber-operations. Taking part in combat action, while carrying on with their civilian life and hiding their status as informational warriors. Making it harder for a state to identify combatants and confine offensive operations to legitimate military targets while avoiding civil society. Potentially resulting in greater suffering as the state uses harsher methods to root out those involved.

So, what can we make of the Iranian Israeli cyber-conflict with Taddeo's insights? First, that rules specifically designed traditional warfare must be adapted to limit the malign influence cyberwarfare could have on future conflicts. Specifically, that cyberwarfare must be included as a last resort, Acknowledging the escalatory nature of these ongoing soft target attacks between Iran and Israel already violate the principle of just cause. That future attacks may only be justified after all reasonable attempts at resolution are exhausted. Second, that destruction of physical objects is not the only criteria to consider when balancing 'more good than harm'. Attacking water treatment, hospitals and petroleum cyber infrastructure should be considered 'physical objects' and weigh just as heavily in that consideration. Third, both Israeli and Iranian civilian's conducting offensive cyber operations should be considered combatants. But care should be taken minimize harm to the non-combatant populace when attempting to identify and root out those individuals.

Deontology focuses on the rules that define accepted behavior and norms making actions that align with those rules ethical and those that do not unethical. This provides a framework that both Israel and Iran can follow as a just war blueprint in future cyber-conflicts. First that both need to make cyber attacks a last resort instead of using it as a form of 'soft conflict.' that abrogates their shared responsibility to exhaust all reasonable efforts at resolution. Second, that hospitals, water treatment and petroleum cyber infrastructure is equal to any physical object and off limits to attacks. Unless clear support of military objectives can be demonstrated, and human suffering demonstrably minimized. At the end of the day, no matter the provocation deontology would teach that if either Israel or Iran is to conduct a just war, they must adhere to traditional principles applied to cyberwarfare if they wish to limit its potential malign influence.

In closing, Boylan and Taddeo's insight into a redefinition of just war as it applies to cyber is needed. State entities run the risk of 'soft conflicts" escalating into open war because neither side acknowledges the dangers in allowing this form of warfare a pass on traditional litmus tests of conflict. Building a culture where a false sense of confidence that actions tantamount to acts of war are somehow ethical and acceptable. This attitude will pave the way for state sponsored cyber attacks to increase in frequency and intensity, escalating in short order to open warfare without any period of resolution or diplomacy. Assuring, that in a states haste to respond, less care will be taken to confine attacks to military targets, spilling over into civilian cyber infrastructure and harming more non-combatants. As was the case between Iran’s targeting of water treatment and a hospital and Israel’s targeting of petroleum distribution.