6.4 Case Analysis on Cyberconflict

Hans Peterson

Old Dominion University

PHIL 355E: Cybersecurity Ethics

Professor Ouabira

April 6, 2026

6.4 Case Analysis on Cyberconflict

Introduction

In the provided article, Veeneman (2023) discusses a new classification of warfare called hybrid warfare, which uses both kinetic and non-kinetic tactics to weaken and defeat an adversary. Kinetic tactics are conventional means of warfare, such as missiles and firearms, while non-kinetic tactics include cyberattacks, information warfare, and supply chain disruptions. These non-kinetic tactics were employed by three hacktivist groups in the start of the Israel-Hamas war, which led to havoc. The cyberattacks from Cyber Av3ngers targeted Independent System Operator, otherwise known as Noga, which is in the electricity industry. Other attacks targeted Israel's missile alarm system, causing it to falsely alert and raise panic, and there were also attacks that targeted Israel's government website and the Israel Electric Corporation, which impacted the function of the Iron Dome system, and this system intercepts incoming missiles for protection (Veeneman, 2023). All of this is to say that cyber-attacks, including information warfare, can cause excessive harm to civilians and non-military targets. It can not only lead to deaths, but it also strains future recovery efforts. Who knows how long these damages will last?

Ignoring the ongoing conflict and its basis, could these cyberwarfare actions be justified in a just war? In this case analysis, I will argue that Kantian deontology shows us that these actions could not be part of a just war because of excessive collateral harm.

Boylan

Boylan presents several important concepts applicable to the previously mentioned article and its debate. One of these concepts is the *just war theory*, which Boylan (2016) traditionally defines as an aggressive act by one against another state's territory or sovereignty to gain land, resources, or a tactical advantage based on international rules/constraints that govern actions both *ad bellum* and *in bello*. Typically, the attacking state is immoral because it caused the conflict. Boylan also mentions "*ad bellum*" and "*in bello*." *Ad bellum*, or *jus ad bellum*, refers to the justification for going to war, and *in bello*, or *jus in bello*, refers to how to ethically conduct the war. This means one can justify war but can also fight the war in an unethical, immoral way (e.g., war crimes).

The issue with cyberwarfare, or even our current conduct of warfare, is not because of a lack of *jus ad bellum* but because our methods of conducting war have exceeded that of *in bello*. To Aristotle, such a just war could only be won through *arête* warriors, or virtuous and excellent warriors (Boylan, 2016). Therefore, a just war was conducted in a virtuous, excellent manner. However, this was an ancient time where war was conducted using cavalry, phalanxes, and swords. Technology advanced, and WWI saw the use of artillery and toxic gas, and WWII saw the culmination of the atomic bomb. These are hardly virtuous weapons, but rather extremely painful and harmful to not only military targets but also civilians caught as collateral. However, these constitute a "traditional" war, where the attacking nation could be identified, and killing/death was expected. Now, cyberwarfare and the cyber-actions employed in the Israel-Hamas war have muddled just war theory. The objective of a cyberattack is primarily not to kill but to disrupt an adversary's systems. An example of this was Stuxnet, in which the targets were Iran's uranium-enriching centrifuges; it only targeted and destroyed these devices. However, cyber-attacks can cause physical harm and even death. An example of this was the

methods used by Cyber Av3ngers and other hacktivist groups. Their main targets were the Iron Dome system, and if it were disabled, incoming missiles would not be intercepted. The disruption or destruction of critical infrastructure not only harms military targets but also does collateral harm to civilians. This is not befitting of the *arête* warriors that Aristotle envisions. These cyberattacks go far beyond what is intended and what actions can be attributed to whom. It would be easy, nowadays, for a cyberattack to occur and for the attacking nation to say that it was another country that did it. There could be an all-out war. Thus, the *jus in bello* can be violated.

Could these cyber-actions be justified in a just war? Using Kantian deontology, these actions can be proven to be unjust even in a just war. According to Kant, it is not the consequences that make actions moral, but instead it is good will, or good intentions. The right action would be the one where you could will as a universal law. If everyone else did it, it would be okay. Additionally, Kant emphasized that the action should not treat people as means to an end, but only as ends themselves. Therefore, the action should not take advantage of people to meet a certain goal. If we applied these to the hacktivist groups involved in the Israel-Hamas war, deontology's principles would be violated. When the hacktivist group, AnonGhost, spammed false Red Alert system missile alerts in Israel, it caused widespread panic in military bases but also in civilian Israeli communities (Veenemen, 2023). Could we will this into a universal law? I doubt that, if every nation used this method to conduct a war, it would be considered fine to the civilians affected by these false alerts. It is also evident that the purpose of these false alarms was to spread terror, confusion, and debilitating panic. The objective was to weaken the adversary government by taking advantage of and terrorizing people. This is hardly

justifiable with Kantian deontology, and it is hardly in line with *jus in bello*. They should, therefore, never be enacted.

Taddeo

Taddeo mentions three important concepts applicable to the article's situation. These three concepts are *cyberwarfare, transversality,* and the *infosphere*. Taddeo (2012) defines *cyberwarfare* as the usage of ICTs in an offensive/defensive military strategy by the state, whose aim is to disrupt an adversary's resources, and it is conducted in an informational environment with participants ranging in physical and non-physical domains and with varying levels of violence. The fact that *cyberwarfare* is versatile when compared to traditional warfare is what makes it different; this can be referred to as *transversality*. In *transversality*, *cyberwarfare* has its own domains (e.g., non-violent, non-physical methods of attacks), but it can also cross traditional warfare's domains in that *cyberwarfare* can easily be violent and cause physical harm to not only military targets but also civilians. Lastly, Taddeo (2012) mentions the infosphere, which is the "environment in which animate and inanimate, digital and analog informational objects are morally evaluated." Under Information Ethics, even inanimate, digital objects, such as websites, have minimal moral rights.

The fact that cyberwarfare is transversal is what makes it more complicated and dangerous compared to traditional warfare. Computer viruses are not inherently lethal or particularly damaging, but if they were designed by a state and unleashed on critical infrastructure (e.g., nuclear power, hydro dams, water treatment), they could pose a larger threat than a gun. Cyberwarfare also does not obey the typical rules that just war theory describes. Bloodless, non-violent cyberattacks, like Stuxnet, still constitute acts of war, and the principle of

war as a last resort can be violated. A cyber-campaign against an adversary can easily lead to a bloody, traditional one. Even then, if an adversary retaliates with a cyberattack of its own, the extent of its damage can surpass the damage that it received. It can be disproportionate. When examining the actions that the hacktivist group took against Israel, they are unjustifiable, and they can easily lead to a worse, physical war. These cyberattacks did not discriminate, and they did not care who was involved (civilian or not). From a certain perspective, it could be argued that it targeted everyone. The cyberattack on Israel's Iron Dome system demonstrated the transversality aspect of cyberwarfare; the disabling of the Iron Dome, though a non-violent action, means the failure to intercept incoming missiles, which are *very* violent actions. The hacktivists' actions did not respect the principles set forth by just war theory and are inexcusable.

Could these cyber-actions be justified even in a just war? Bearing in mind the concepts that Kant mentioned in his argument for deontology, the cyber-actions still cannot be justified. Justification is even worse when Taddeo's concepts of the Infosphere and Information Ethics are applied to the hacktivists' actions. Again, the Infosphere includes any inanimate, digital object in the environment, which includes e-books, websites, and movies. Under information ethics, these objects deserve moral rights and are to be treated equally to living things: they have a fundamental right to exist. Therefore, to protect the Infosphere, entropy (e.g., destruction, depletion, corruption) should not be exposed to the Infosphere. All actions toward entropy are to either remove, prevent, or refrain from bringing it to existence. When we splice in Kant's emphasis on not taking advantage of people as tools, the hacktivists' cyber-actions become indefensible. These cyberactions, such as the takedown of the Government of Israel's website and the impact of the Iron Dome system, introduce entropy into the Infosphere. If we treat these digital objects as equal to living things, as prescribed by information ethics, it can be argued that

these cyber-actions took advantage of "living things," which goes against deontology's principles. All in all, the hacktivists' actions are unjustifiable and should have never been enacted.

Conclusion

Because of the excessive collateral harm that the hacktivists' actions would bring to civilians and digital objects, these cyberwarfare actions cannot be justified even in a just war. These cyberwarfare actions do not fit into Boylan's concept of jus in bello, and neither do they fit into Taddeo's Infosphere and the principles set forth by Information Ethics. There are wider implications beyond this case. Going back to Stuxnet, the consequences could have been worse; considering the transversality of cyberwarfare, Iran's retaliation could have been violent, or further cyberactions could have escalated in terms of nondiscriminate damage. Additionally, it could also be argued that Stuxnet violated information ethics principles, such as the introduction of entropy. The Infosphere also includes inanimate, analog objects, something as simple as a tree or rock. Under this broad inclusion, Iran's centrifuges in their uranium enrichment facilities are protected objects part of the infosphere. This would also mean that future cyberwars will essentially be violations of the Infosphere, as the main objectives of cyberwarfare are to disrupt, destroy, or control adversary systems. Regardless, cyberwarfare actions will introduce entropy into the infosphere.

References:

Boylan, M. (2016). *Can there be a Just Cyber War?* Philpapers.org. https://philpapers.org/rec/BOYCTB

Taddeo, M. (2012, June 1). *An analysis for a just cyber warfare*. IEEE Xplore. https://ieeexplore.ieee.org/document/6243976

Veeneman, P. (2023). Digital Battlegrounds: Evolving Hybrid Kinetic Warfare. *Industrial Cyber*. https://doi.org/10/2023.10.12-Digital-Battlegrounds-Evolving-Hybrid-Kinetic-Warfare