Ray Tischio
Final Essay for THEO 4026
Professor Father Massaro
Fall 2019

Fitting *the Just War Theory to* the Fifth Domain*:* Is Cyberwarfare Any More Ethical?

In light of completing my International Studies thesis on nation-state cyber conflict this semester, I have given a lot of thought to the ethical component of this subject throughout the last few months. Although ethics was not something my thesis particularly addressed, I often found myself naturally applying relevant discussions and concepts taught in other courses to the matter that I was focusing on in my research; specifically, learning about approaches to just war in the course *Theologies of Peace* provoked my contemplation of the ethical component to cyberwarfare. Thus, I saw this prompt as an opportunity to continue considering and weighing the ethical challenges surrounding cyberwarfare. In this essay, I will apply the Just War Theory and its *jus ad bellum* and *jus in bello* conditions to broad aspects of cyberwarfare, while juxtaposing some of cyberwarfare's fundamental qualities with those of conventional kinetic battlefield warfare. In doing so, I'll articulate *new* challenges, if any, that cyberwarfare poses to the JWT's method of defining an ethical use of force.

As a domain of warfare which has only significantly emerged in the last decade, there remain gaps in international legal framework for dealing with and responding to the threat and force of cyber operations. Cyber conflict includes offensive capabilities, such as cyber exploitation (obtaining confidential information through cyber means, often unauthorized access or penetration of networks) and cyberattacks (degrading, disrupting, or destroying a system or information).[1]

My chosen metric for evaluating the ethics of cyber conflict is the Just War Theory (JWT), as it attempts to comprehensively define morally justifiable war through a set of criteria and conditions which must be met in order for a war to be considered just. In addition, this theory incorporates several principles regarding diverse features of the use of force and military aggression. The JWT is rooted in philosophy and history; dating back to the ages of Greek and Roman philosophy, it began with the ideas of Plato and Cicero. However, the just war *tradition* has developed from this and become a focus of Christian theology as well, with prominent figures such as Ambrose and Augustine having contributed to its development.[2] In the following paragraphs, I will outline some of the main tenets of the just war theory while applying it to corresponding elements of cyber conflict.

The JWT begins with the principles of *jus ad bellum*: 1) just cause, 2) legitimate authority, 3) just intention, 4) last resort, and 5) probability of success, all of which address when it is permissible to go to war. When scrutinizing cyber conflict in the context of these principles, there is some contradiction. Firstly, the *cause* behind cyber conflict generally is not in "national self-defense or protecting the weak and vulnerable," and thus may not be considered just according to the just cause principle.[3] Rather, cyber operations are largely in the self-interest of

[1] Herb Lin, "Fundamentals of Cyber Conflict," *Stanford University,* (May 2017), https://seclab.stanford.edu/courses/cs203spring2017/lectures/lin.pdf

[2] Joseph S. Fahey, *War and the Christian Conscience: Where Do You Stand?* (Maryknoll, NY: Orbis Books, 2005), 86-108.

[3] Mark J. Allman, *Who Would Jesus Kill? War, Peace, and the Christian Tradition* (Winona, MN: St. Mary's, 2008), 167.

the state. In the short history of cyber conflict, its motivations do not include humanitarian intervention, or R2P, as they often do in the case of kinetic war. The *just intention* clause raises similar questions. According to it, peace is "the only legitimate end that one can seek" in committing to acts of aggression, "since peace is the goal of war."[4] However, cyber conflict is largely a game of ulterior motives and geopolitical power plays, ranging from expanding spheres of influence in a region, seeking revenge on another nation, or bolstering a domestic economy. Inherently, these ulterior motives are quite unpeaceful. Its goals differ from those of kinetic war. The *legitimate authority* principle highlights the difference between cyberwarfare and conventional modes of battlefield warfare. In the history of state cyber conflict, not only do governments not declare their intended actions prior to executing cyberattacks, but they often attempt to divert attribution and mask themselves as the source. By the definition of this clause, no historical example of cyberwarfare could be defined as just due to its clandestine nature; however, perhaps a future version of a theory tailored to cyber conflict could address this unique challenge that this mode of war presents.

Applying both the *last resort* and *probability of success* principles produces a similar outcome. Both illuminate the futility of many cyber operations based on the definition of just war. These operations are arguably unnecessary, and rather provide a means for a state to act on self-interested objectives; clearly, they are not a last resort. Similarly, cyber conflict would be considered futile due to the definition of success here in terms of resolving conflict, and having a "positive influence on the situation."[5] Cyberwarfare serves no real purpose in attaining peace or

[4] Allman, 168.

[5] Allman, 198.

reducing future conflict. If anything, it holds the potential to sour nation-state relationships and threaten existing bilateral stability. As these clauses also challenges the possibility of labelling cyber conflict just, they remain important to an overall understanding of morality in contrasting modes of warfare.

The second major portion of the JWT is that of the *jus in bello* principles: 1) proportionality, 2) discrimination, and 3) legitimacy of targets, all of which address what is morally right or just behavior during war. The first condition, proportionality, limits the amount of just force to only that which is proportionate to the intended objective;[6] this raises an interesting differentiator between cyber and kinetic warfare. The role of physicality is important here in our notion of force and impact. Cyber conflict has not (yet) escalated to the point of mass casualties, as is common in battlefield warfare; however, the objective acted on - even if to merely disrupt other nation's infrastructure - must be included in our assessment of ethics here. Because the realist-driven goal of projecting one's own power and dismantling the power of another is inherently not just according to the JWT, can this form of even non-lethal force be considered ethical? Perhaps even disruption to network systems and systematic espionage could violate this principle of proportionality.

The *discrimination* clause declares that a just war must distinguish between "soldiers (combatants) and civilians (noncombatants),"[7] but as other critiques of the JWT have stated, this principle is difficult to apply to even modern forms of guerilla warfare and counterterrorism as it is much harder to distinguish between soldiers and civilians than it was in large-scale military

[6] Allman, 204.

[7] Ibid, 200.

battles, which were more common at the time of the JWT's conception. Introducing cyberwarfare into the application of this principle further removes its relevancy. Along with not having necessarily traditional soldiers execute state-sponsored cyberattacks, the problem of attribution again renders it largely unclear who is conducting what in cyberspace. However, the *target legitimacy* condition remains a pertinent point in deciding ethics of cyberwarfare. Today, cyber operations do threaten critical national infrastructure (CNI). Communication and financial networks along with electrical power grids are among common targets of nation-state cyberattacks. In fact, actual blackouts have occurred due to one state's remote shutting down of another's power grids, sending hospitals and other emergency services offline. This raises questions about objectives of cyberwar, and may point to critical areas that need to be immediately addressed by theories such as an updated version of the JWT, and international agreement.

In this brief attempt to fit the JWT framework to the emerging domain of cyberwarfare, I reach several interesting conclusions. Firstly, the instinct to declare cyber conflict as more ethical due to its lack of producing a death toll or physical destruction, for example, is clearly not supported by this analysis. As is revealed in this essay, the JWT focuses heavily on moral and necessary intentions behind the use of force, a condition with which the current demonstration of state cyberwarfare does not align. Similarly, the JWT is concerned with clear definition and limited use of war, which again, is not the current reality for the grey, murky area of interpreting and assessing cyber conflict. However, it could be argued that the common execution of cyberwarfare cannot be classified as just according to the JWT. Cyberattacks are not used to fight for peace or defend the common good, but rather for acting on state objectives. As the morality of the JWT is still sound, it is at the very least evident that this age-old theory cannot be readily prescribed to fit the new challenges of the fifth domain. As a global community filled with interdisciplinary knowledge, we must work to build a framework that does address these discrepancies, and continue to promote the peace-seeking morality even in efforts involving warfare.

Bibliography

Allman, Mark J. *Who Would Jesus Kill? War, Peace, and the Christian Tradition.* Winona, MN: St. Mary's, 2008.

Fahey, Joseph S. *War and the Christian Conscience: Where Do You Stand?* Maryknoll, NY: Orbis Books, 2005.

Lin, Herb. "Fundamentals of Cyber Conflict." *Stanford University.* May 23, 2017. https://seclab.stanford.edu/courses/cs203spring2017/lectures/lin.pdf