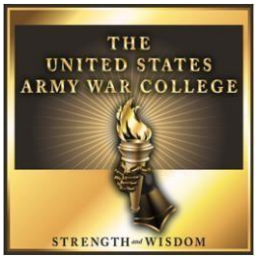
Strategy Research Project

Justified Physical Response to Cyber Attacks from Walzer's Legalist Paradigm

by

Commander Joseph W. Smotherman
United States Navy

Under the Direction of:
Chaplain (Colonel) John Kallerson



United States Army War College
Class of 2016

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2016	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Justified Physical Response to Cyber Attacks from Walzer's Legalist Paradigm

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Commander Joseph W. Smotherman
United States Navy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Chaplain (Colonel) John Kallerson

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
Please consider submitting to DTIC for worldwide availability? **YES:** ☒ **or NO:** ☐ **(student check one)**
Project Adviser recommends DTIC submission? **YES:** ☒ **or NO:** ☐ **(PA check one)**

13. SUPPLEMENTARY NOTES
Word Count: 5730

14. ABSTRACT
As warfare evolves, new technology pushes the limits of acceptability and operations in cyberspace are no different. If attacks in cyberspace are assaults of one state against another, then the framework of Just War theory should still apply and Michael Walzer's Legalist Paradigm provides a clearer lens on when an armed response to a cyber attack is morally permissible. While some parts of Just War theory directly apply to responses to Cyber Attacks, the others do not, beginning with Just Cause. Walzer describes Just Cause in terms of the natural rights of the citizens of a state, and when a cyber attack interrupts the ability of those citizens to make a life together or the "safe space" they create, then a physical response to a cyber attack could be justified. This paper outlines the relationship between Walzer's Legalist Paradigm and justification for physical responses to cyber attacks, with the intent of providing senior leaders with a framework for those responses.

15. SUBJECT TERMS
Just War Theory, Cyberspace Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	26	

Justified Physical Response to Cyber Attacks from Walzer's Legalist Paradigm

(5730 words)

Abstract

As warfare evolves, new technology pushes the limits of acceptability and operations in cyberspace are no different. If attacks in cyberspace are assaults of one state against another, then the framework of Just War theory should still apply and Michael Walzer's Legalist Paradigm provides a clearer lens on when an armed response to a cyber attack is morally permissible. While some parts of Just War theory directly apply to responses to Cyber Attacks, the others do not, beginning with Just Cause. Walzer describes Just Cause in terms of the natural rights of the citizens of a state, and when a cyber attack interrupts the ability of those citizens to make a life together or the "safe space" they create, then a physical response to a cyber attack could be justified. This paper outlines the relationship between Walzer's Legalist Paradigm and justification for physical responses to cyber attacks, with the intent of providing senior leaders with a framework for those responses.

Justified Physical Response to Cyber Attacks from Walzer's Legalist Paradigm

As the character of warfare evolves, new technology continues to push the limits of acceptability. The consequences of warfare in the cyber world do not fit neatly into society's paradigm of right versus wrong and what is just. Despite the old adage, not all is fair in war. In the rapidly developing world of cyberspace, each action will push the boundaries of propriety. Questions that previously had easy answers are no longer black and white: When Saddam Hussein's Iraqi Army pushed across the border on August 2, 1990, there was no doubt that his aggression was a cause for war, but today, if one country were to use attacks in cyberspace to cripple the infrastructure of another, the decision to retaliate is not so clear. All states should reserve the right to respond to a cyber-attack with force as a deterrent, and the United States has stated that it will consider physical responses to cyber attacks. Deputy Defense Secretary William Lynn said "The United States reserves the right, under the laws of armed conflict, to respond to serious cyberattacks with a proportional and justified military response at the time and place of its choosing."[1] If a nation (not just the United States) must decide when to respond to a cyber attack with physical force, then an appropriate framework must be established for cyber attacks as armed attacks. If cyber attacks are assaults by one state on another then the Just War framework should still apply, and as a more contemporary conception of Just War, Michael Walzer's basic premise of the Legalist Paradigm provides a clearer lens on when an armed response is morally permissible. When examined in terms of political sovereignty and territorial integrity, cyber attacks can be a form of aggression and, therefore, just cause for war.

Attacks using cyber warfare have been examined from the perspective of the Law of Armed Conflict, and legal guidelines have been established. In spite of this,

when a cyber attack occurs, the leadership of the victimized country must decide when a physical response is justified.[2] This paper will explore when that is the case. The first section will describe the cyber domain and make the distinction between operations in the cyber domain and cyber attacks. Following the discussion of the cyber domain, it will give a brief primer on classic Just War Theory (JWT), followed by an examination of the application of JWT to cyber attacks through the lens of Michael Walzer's Legalist Paradigm and theory of aggression put forth in his book, *Just and Unjust Wars*. The discussion of JWT theory will begin with the aspects of JWT that are straightforward, regardless of the nature of the attack. It will continue with an analysis of just cause, as that is the lynchpin of the last three criteria. After a determination of just cause, the final three criteria of JWT will be evaluated in the context of whether or not the cause for retribution is sufficient.

Operations in Cyberspace

"Cyber" is a new aspect of the modern battlefield. Its evolution and arrival follows the Clausewitzian construct of the nature and character of war: The use of cyberspace in war is a new tool and method of fighting (the "character of war") with the end of forcing an enemy to bend to the attackers will (the "nature of war").[3] Because of the futuristic aspect of "cyberwar," it becomes a phrase that is used in parlor discussions without sufficient specificity and is often shortened to just "cyber."[4] For the sake of clarity, all definitions used will be based on the definitions found in Department of Defense Joint Publications. The first and most basic definition is that of cyberspace. Cyberspace is "A *global domain* within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded

processors and controllers. [Emphasis added]"[5] The highlight of this definition is that cyberspace is a domain: "a sphere of knowledge, influence, or activity."[6] Cyberspace becomes a location, albeit virtual, on par with the maritime, land, air, and space domains. Operations conducted in cyberspace are "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace operations (COs) are composed of the military, intelligence, and ordinary business operations of DOD in and through cyberspace."[7] In short, cyber operations are any activities that take place in cyberspace, whether day-to-day activities or attacks. Cyber Operations can take on many forms. They can take the form of Information Operations (IO), or they can be full-fledged cyberspace attacks. In the past, all CO were considered subsets of IO, but have recently been separated as a unique form of warfare.

For the purposes of this discussion, it is important to separate cyberspace attacks from other operations conducted in cyberspace.[8] Cyberspace attacks are those operations in cyberspace "that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains."[9] If the actions taken in cyberspace are not intended to deny or manipulate an adversary or enemy's capability, then they are not attacks. Another definition is offered in the Tallinn Manual, a description of international law's application to attacks in cyberspace published by NATO's Cooperative Cyber Defence Centre of Excellence.[10] The Tallinn Manual defines an attack as "a cyber operation, whether offensive of defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[11] As

an example, the data stolen from defense contractors Boeing and Lockheed-Martin by Chinese hackers would not qualify as an attack due to the intent to acquire information rather than deny or manipulate U.S. systems.[12] As an analogy, a physical operation with the same effects would simply be espionage: treated as a criminal enterprise rather than a use of force.

Because of the relatively low entry cost to the cyber domain, it is accessible to many different actors, which contrasts with the assumption of classic JWT that war is an activity between established states.[13] In the modern world, there are non-state actors who take part in war-like activity, but warfare in its classic sense is still the providence of states, as evidenced by the United States quandary in dealing with fighters captured in the Global War on Terrorism. They do not represent any state and are therefore not subject to any of the moral or legal protections of warfare. In any case, a physical, armed response to non-state actors is still an act of war against the state in which they reside and any physical response to cyber attacks must be considered in the same fashion. An analogy with the war in Afghanistan holds: the United States entered into war with the ruling Taliban because of their relationship with al Qaeda. If a non-state actor (or actors) performs an act of terrorism or a cyber attack, any response against that actor in their location becomes an act against that state. Additionally, it could be expected that two states previously in a state of war would not have any moral quandary when deciding to respond to any attack with force. Because of this, examining responses to cyber attacks through the lens of non-warring states provides clarity as a starting point, but extrapolation from state on state attacks to non-state actors become more closely aligned with recent principles developed in the Global War on Terrorism.

New problems sometimes do not require new principles as much as they require an examination of the basics.

As a working definition, the Tallinn Manual is most restrictive, but it also leaves open the possibility of an adversary "working around the edges" by using temporary effects. The U.S. Department of Defense Joint Doctrine on Cyber Operations, Joint Publication (JP) 3-12 definition considers both intent (denial or manipulation) and permanent or temporary effects that may remain hidden or exist in the physical realm. Consequently, the JP 3-12 definition is more complete and allows for both deontological and teleological consideration of an attack.[14] Unfortunately, neither the Tallinn Manual (as an examination of international law) nor U.S. military joint doctrine gives adequate instruction for cyber attacks that do not have physical effects but leave the leadership and populace of a country with the sense that a strong response is required.

Just War Theory

The basis for international law surrounding the conduct of war began with the philosophical Just War Tradition that traces its roots to Aristotle, Cicero, and more popularly, Augustine.[15] Over the course of time, this tradition has been considered from three perspectives: *Jus ad bellum, jus in bello*, and *jus post bellum*. These phrases persist in both Just War tradition and in international law and each have specific conditions.[16] For the purposes of this paper, we will only discuss *jus ad bellum* (conditions for going to war).

The beginnings of a coherent Just War Theory were articulated by Saint Thomas Aquinas in *Summa Theologica*. He addresses what are generally considered to be the first three conditions necessary for a war to be "just:"

1. War must be declared by a nation state (*legitimate authority*).

2. There must be a *just cause* for which the war is being fought.

3. The intent of fighting must be morally worthy as well (*right intention)* Later scholars added other criteria.

4. War must be a *last resort*.

5. There must be a *reasonable likelihood of success*.

6. The cost of fighting a war must be proportional to the wrong to be redressed (*proportionality of ends*).

7. Any war must not only be just in its cause, but also fought with *just means* (*jus in bello*).[17]

The *jus in bello* criterion is sometimes separated from the broader *jus ad bellum*. *Jus in bello* applies to the individual soldier fighting the war, but it also applies to those directing the war in a larger sense. For the purposes of cyber-attacks, it is important to consider that any actions must conform to *jus in bello* criteria as a whole, even though *jus in bello* is beyond the scope of this paper.

Many of these criteria apply to attacks in cyberspace in much the same fashion they do to physical attacks (legitimate authority, right intention, probability of success) , but others (just cause, last resort, proportionality of ends, and just means) are more difficult to shape because of evidence of an attack. In a world of physical warfare, it is easy to point to the effects left behind by any act of aggression. In a cyber attack, the only evidence may be the destruction of information (or financial, or in some cases critical infrastructure that continues to malfunction with deleterious effects). While the first three criteria of Just War Theory (legitimate authority, right intention and probability of success) are essential, they change very little for responses to a cyber attack. A state, rather than individuals acting alone, must respond in a fashion aligned with moral ends and be likely to achieve them.

Directly Applied Aspects of Just War Theory: Legitimate Authority, Right Intention, and Reasonable Chance of Success

The question of legitimate authority is easily applied, even to attacks waged in cyberspace. Since war is an activity, an armed conflict, between political entities it requires that those engaging in such activities represent such an entity.[18] The most common is the state, but an insurgency can represent populations as well. The pre-Westphalian world of Saint Thomas Aquinas did not recognize states as we know them; war was waged by and between princes. These princes controlled territory and were political rulers, and today this concept has evolved into the modern states. Modern day war remains an activity between those states. A state (and since only a state may wage war) that desires the moral and legal protections of *jus ad bellum* must be a recognizable (if not recognized) political entity. Otherwise, any response is simply a criminal activity to be dealt with internally.[19]

Right Intention is an issue that applies to responses to cyber attacks in the same manner as traditional, physical uses of force. The intent of any response to a cyber attack must be morally just. While this requirement follows from just cause, one state must act with an intent that, if motivated during any other form of warfare, would still pass the test. The ways, or manners, of response become less important.

As with any type of attack, one must be able to expect a reasonable chance of success. Whatever the espoused cause and desired ends of a response, there must be some chance that it may be successful, and must be related to proportionality of ends. While this criterion does not demand certainty of success, the degree of surety of a desired outcome must exist to the same degree as an attack for any other form of aggression.

The Central Problem: Just Cause

While the previous demands of Just War Theory change little for attacks in cyberspace, the others are not so clearly defined. Just cause, last resort, and proportionality of ends are all more difficult to apply when dealing with attacks in cyberspace. One of the most prominent political philosophers currently considering contemporary issues in Just War Theory is Michael Walzer.[20] In his book, *Just and Unjust Wars,* Walzer attempts to refine the Just War Theory for modern times. The most profound outcome of his book was an attempt to define just cause in terms of the natural rights that man binds together in states to protect: rights such as life, liberty, and property. War is justified when those natural rights are threatened.

In the cyber domain, the most problematic of the classic Just War Theory criteria for waging war is just cause. Early Just War Theorists such as Augustine of Hippo approached the warfare from the pacifist beginnings of the Christian Church, where killing was prohibited, but war became a necessary evil in order to govern the empire as Christianity spread.[21] This is considered the most important of the criteria, and a foundation for every other criteria. This often is broken down into two separate categories of “wrongs received:” self defense and punishment for a grievous, uncorrected wrongdoing.[22]

The first of these, self-defense, is viewed as the *only* just cause for war in international law in which a state may take unilateral action.[23] This right of self-defense applies not just to a country protecting itself, but also includes collective self-defense: the defense of other states.[24] Philosophers have long attempted to define the bounds of self-defense, and when applying “self-defense” to cyber attacks, it becomes even more difficult. How does one determine self-defense when there are no invading armies? Can

a war waged against a state that does not cross into another's territory be considered self-defense? These questions become more critical in an age of expeditionary warfare. The United States, for example, has not fought a foreign nation on her shores since the Mexican American War in the 1840s, but the United States has fought in wars that were considered "just." As an example, the beginning of the current conflict in Afghanistan is generally considered a just cause, but the government of Afghanistan did not invade the United States in the traditional sense. That government, on the other hand, offered aid and protection to those who attacked the U.S.

The second traditional cause for just war is the punishment of a state for some wrongdoing. The framework for punishment as just cause has always been problematic. Very little has been agreed upon, either in customary or international law, or even the basic premise behind what this punishment is intended to accomplish.[25] Walzer describes it simply as the international analogue to punishment for domestic crime: to prevent future aggression.[26]

Unfortunately, cyber attacks do not fit nicely into either of these categories. Even if a cyber attack has the same effects as an armed attack (perhaps an attack commands infrastructure to destroy itself and causes the deaths of a large number of people), it is still difficult to declare that as an attack requiring defense if there is no realistic threat of continued action that an armed physical response would interrupt.

Michael Walzer provided a new, modern way of thinking in *Just and Unjust Wars.* His different perspective provides a paradigm of applying Just War Theory that when applied to cyber attacks, helps define just cause in a clearer fashion. In the fifth edition of *Just and Unjust Wars,* Walzer link his specific theory to traditional Just War Theory,

saying “there is no reason why it can’t work”[27] in current times and explains that his is an attempt to describe the new character of war as it relates to Just War Theory. His question (and answer): “Do the same rules apply [to asymmetric war]?[28] I want to say that they do, but that requires an argument.”[29]

Walzer’s argument in *Just and Unjust Wars* is centered on what he refers to as the “Legalist Paradigm.” The basis for this argument is that just cause for war is the maintenance of law and order in the international realm. In Walzer’s world, the *only* crime that a state may commit is termed “aggression.”[30] He compares it to domestic crimes, and lists a range of different categories among individuals, but when a violation of international rights occurs there is no other name for it than simply “aggression.” The comparison of violations on an individual level and an international one is what Walzer terms the “Domestic Analogy.”[31] This analogy leads to the *Legalist Paradigm* and has six propositions.

1. There exists an international society of independent states.
2. The international society has a law that establishes the rights of its members—above all, the rights of the territorial integrity and political sovereignty.
3. Any use of force or imminent use of force by one state against the political sovereignty or territorial integrity of another constitutes aggression and is a criminal act.
4. Aggression justifies two kinds of violent response: a war of self-defense by the victim and a war of law enforcement by the victim and any other member of international society.
5. Nothing but aggression can justify war.
6. Once the aggressor state has been militarily repulsed, it can also be punished.[32]

Since states are the collectivization of the rights of their citizens, then a state must have a claim to natural rights, a concept drawn from John Locke's writings on the nature of government. The two primary forms of these natural rights for a state are territorial integrity and political sovereignty. Any threat to either of the conditions is a threat to the state and constitutes aggression: the only just cause for war. When viewed from the perspective of territorial integrity and political sovereignty, then cyber attacks can be aggression and just cause for war.

According to Walzer, since the members of the international order are states, and he asserts that the only crime a state may commit against another state is aggression, and that is "the name we give to the crime of war."[33] While aggression may be fighting, whether in a warring or other sense, the key to identifying aggression is that it interrupts the peace. "Peace" in this sense is not a world without fighting, but "peace with rights, a condition of liberty and security that can exist only in the absence of aggression."[34] The crux of Walzer's theory of aggression is that people band together to form states, and these states represent the collective natural rights of its citizens: "the duties and rights of states are nothing more than the duties and rights of the men who compose them."[35] These duties and rights are the natural rights Americans are familiar with from Locke's natural rights of man: life, liberty, and property (possessions).[36] Walzer declares threats to these rights as simply "aggression." Life and liberty in their collective form are political sovereignty and the collective property is territorial integrity. The political sovereignty is a long established contract: rather than a "transfer" of rights, the state protects the common lives of its citizens, which gives the state a moral standing to exist. If the state will not protect its citizens, then it loses that moral standing.[37] In addition to protecting

political sovereignty, the state must also guard its territorial integrity. While protecting territorial integrity is not the same as ownership, Walzer compares it to the individual's right of property even in a home that she does not own. She must have some place safe from intrusion, and the existence of a state provides that space.[38]

As cyber technology continues to integrate with every aspect of daily lives, the likelihood of two adversaries using cyber operations to wage a war against each other grows. This is especially true if one side has a distinct military disadvantage but desires a first strike or feels that a preemptive strike is justified.[39] Some legal writings, most notably the Tallinn Manual, consider only the physical effects of a cyber operation: if the effects are comparable to a non-cyber attack, then it may be considered an armed attack.[40] While this is an excellent starting point for identifying aggression, very few cyber attacks will "look like" a physical armed attack in their results. A bomb leaves a large crater, while a cyber attack may leave all equipment in place but in a non-working status. Evaluating these attacks from Walzer's Legalist Paradigm and determining if an attack violates the natural rights of a state in the form of political sovereignty and territorial integrity, its "life, liberty, and property," will help clarify whether these cyber attacks that may not leave a "smoking hole" constitute aggression.

Many cyber attacks are attacks on the political sovereignty of a state. The right of a people to be free from foreign "control and coercion"[41] is the keystone of political sovereignty. In a conventional war ideal, this would seem to mean physical occupation or perhaps even an assassination of a leader by a foreign nation, although if "assassination tends to become the norm of political affairs--indeed, civil politics would thus crumble into fearful and barbaric plots and conspiracies (as did Rome in its last

centuries) in a race to gain power and mastery over others rather than to forge justifiable sovereignty."[42] In the world of cyberspace, attacks may take many forms with the intent of coercing and controlling the targeted group with behavior change. In the extreme, a cyber attack could be used to install a government favorable to an adversary. This is a circumstance to which a liberal democracy would be especially vulnerable. In other cases, this could take the form of an attack to terrorize a population in the way it institutes or enforces laws.

Recently, a foreign entity tried to use cyber operations to coerce a corporation not to market a product it had created. In November 2014, the computer network at Sony Entertainment Pictures was penetrated by hackers. These hackers, calling themselves the "Guardians of Peace" demanded that Sony stop the release of *The Interview,* a comedy critical of North Korean leader Kim Jong Un. If Sony released the film, then the Guardians of Peace would publicize documents and emails embarrassing to Sony officials and employees. The FBI attributed the attack to the North Korean government, and confirmed that it was in response to the film.[43] While this example is directed at a private sector company, government officials could be just as, if not more, vulnerable to such embarrassing revelations, especially for elected officials that must guard their reputation for upcoming elections.

Take the example of the 2007 Estonian Distributed Denial of Service where online systems in Estonia were rendered useless in a cyber attack.[44] This attack was a response to political action to move a memorial to Russian soldiers from World War II. While the attack was never fully attributed to anyone specifically (it originated in Russia, but it was not clear if the attack was the act of individuals or sponsored by the Russian

government), it was a clear attempt to coerce the Estonian government and people to change their intended action by outside individuals, a clear assault on the internal political sovereignty of Estonia.[45]

While the use of a cyber attack to indirectly influence the internal workings of a state are easiest to imagine, there is the possibility of more direct involvement. As technology inserts itself as a vehicle for the democratic process, an ill intended actor could use technology to influence the political process through direct means. It would be conceivable that a cyber attack could actually change the outcome of an election with an aggressor installing a government favorable to itself. In the 2016 election, caucus chairs in both Iowa and Nevada reported results using a specially designed Microsoft smartphone application.[46] Imagine the chaos that would follow if a vote count was changed. The faith in decisions for a nation would be shaken to their core, especially in a democracy that relies on the consent of the people to follow the rule of law rather than being ruled by an authoritarian government. Any of these examples, in the proper circumstances, could represent an attack on the political sovereignty of a state and therefore, aggression against them.

The clearest form of aggression is a violation of territorial integrity. While the prototypical ideal of a violation of territorial integrity would be an invasion with great armies crossing borders, it is not simply about the possession of land. Territorial integrity is a function of national existence. It is the “coming together of a people that establishes the integrity of a territory.”[47] In the earlier analogy about a house being robbed, it is about the safe space a nation creates for itself. When a cyber attack occurs, it threatens that safe space. Just as in our own homes we assume we are safe

from intrusion, we should be able to assume that activities that occur within our state will be allowed to continue. If that safe space is violated, then the method used to perform the intrusion is of less concern than the intrusion happening in the first place.

In remarks to the United States Cyber Command Interagency Legal Conference, Harold Hongju Koh referenced

> [c]ommonly cited examples of cyber activity that would constitute a use of force include, for example, (1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction, or (3) operations that disable air traffic control resulting in airplane crashes.[48]

While Mr. Koh was discussing these attack in a legal sense, he is picking examples that are clear uses of force, but do not involve a direct violation of territorial integrity in the sense of foreign invaders. On the other hand, they are still violating Walzer's "safe space" concept. As one begins to explore less clear examples in terms of violence, the domestic analogy becomes more important. It is fair to expect that property, equipment or possessions are not in jeopardy[49] when fairly acquired and safe within a state's territory.

A recent example of a cyber attack destroying property is the Stuxnet virus: a cyber operation against Iranian nuclear enrichment centrifuges. The virus consisted of malware that replicated itself on computers and media with which it came in contact. The virus was limited in duration and number of times it would replicate, and it searched for a specific combination of software on the infected computer in order to target the specific controllers for the Iranian centrifuges. When the conditions were met, the virus caused the centrifuges to spin out of control, thereby destroying them and the uranium they were enriching. Ryan Jenkins, in his 2013 article in *Journal of Military Ethics* article describes this not as an invasion of physical space, but rather an invasion of Iran's

cyber territory.[50] While this may be confusing at first glance, it follows the idea of the safe space: digital infrastructure is the cyber territory that should be regarded in the same fashion as physical territory. The expectation is that property (whether the individual's property or the state's) should be safe within these territories, much as Walzer's analogy of territorial integrity is the collective right of a home's resident to not expect her possession to be in jeopardy. Jenkins also compares this destruction to a special warfare-style raid on the facility.[51] The circumstance that the territory was invaded by electronic instructions on a computer rather than individuals with weapons is less important than the safe space that was violated.

Following from Just Cause: Proportionality of Ends and Last Resort

As one state violates the sovereignty of another and the victim of this aggression considers a response, the "good" of the response must be compared to the "wrong" received. These positive effects must be considered in terms of the overall effect: not simply from the perspective of the state pursuing the action.[52] In other words, a state may not wage war for any triviality. While this concept holds for responding to cyber attacks, it is difficult to apply the ideals directly. If an attack is simply a nuisance: a Denial of Service attack that makes the internet run slowly, it is hardly proportional to create the evils of war simply because life is made difficult. The problem of proportionality is ever present, but cyber exacerbates the concern. Decisions to go to war are clearer when counting bodies, but become less so when deciding if it permissible to destroy infrastructure, causing suffering, or killing people simply because electronic data was manipulated on a computer. Responses are less clear when results look like a physical attack, but no loss of life happens: a power supply is taken down, the banking or financial institutions are destroyed, the water supply is polluted, or

aircraft are grounded because they cannot be controlled safely. All of these are effects of attacks that could happen with a physical attack or by using electronic means. In any of these cases the means of the attack is less important than the effect they have on a population: attacks in cyberspace must be framed in terms of their effects, rather than the means used. Additionally, since the proportionality clause is concerned with ends desired compared to evils present, the actors must consider the degree to which cyber attacks are ongoing and if any retaliation would stop attacks. Furthermore, will any retaliation prevent future attacks?

While concerned about proportionality regarding the short term effects of a response, one must also consider the long term effects. Will an immediate response lead to a larger war? The means of response may change how any response is perceived.

If one state is considering a physical response to any attack, then this decision to wage war must not be taken lightly. While the ends must be proportional, then it should also not be done as a first choice. Another *jus ad bellum* condition is that war must be a last resort. If killing in war is abhorrent, one must ensure that there is no other response that is appropriate. In many modern conflicts, the parties involved are at tensions for some time prior to any actual conflict. Orend describes the simplest definition: "when it seems the last practical and reasonable shot at effectively resisting aggression."[53] Orend's conception is direct, but it leaves much to the judgement of the actors with very little guidance. Walzer discusses the idea of last resort in the context of preemptive attacks, but he gives a clearer framework that aligns nicely with the Legalist Paradigm and, by extension, just cause. "States may use military force in

the face of threats of war, whenever the failure to do so would seriously risk their territorial integrity or political independence."[54] While Walzer's definition still requires some degree of reasoned judgment, it does give a framework: if action is not taken, would an actor commit aggression, or continue to commit it in the case of ongoing attacks?

From the perspective of the cyber domain, if an attack is ongoing, and the only way to stop that attack is through a physical response as opposed to cyber defense, then that is clearly an acceptable case of last resort: it is an emerging act of aggression that cannot be stopped otherwise. On the other hand, if there is not continuing aggression in the cyber domain the decision is more challenging, but should be able to answer the following question in the affirmative: Would failure to act leave political sovereignty or the safety of cyber territory under threat in a reasonable horizon? If the answer is no, then any response does not likely pass the test of last resort.

Conclusion

For a leader that is responsible for the collective rights of their population, a decision to carry out an act of war, especially one that changes the character of a conflict from a cyber war to a physical one, cannot be taken lightly. These leaders must decide when it is both moral and legal to respond physically to a virtual attack. A slight change in the perspective will make it a clearer description, and using Walzer's logic and reasoning clarifies the ideas of territorial integrity and political sovereignty in to a more tangible approach. When the cyber domain is viewed as cyber territory, and the effects are considered in relation to their effects on Walzer's

description of a state's "safe space" (territorial integrity) or ability to govern itself (political sovereignty), a leader can articulate when it is appropriate to attack another nation after being victimized by in the cyber domain.

As technology continues to advance, the ability of aggressors, whether nation states or individuals, to attack other nations with nothing but electronic means will only increase. The effects of these attacks will have more and more profound consequences to the victims, even if there is no death and destruction. Nations will need to continue to determine how they will respond to such attacks. The most elemental question in future world of cyber attacks will be if these attacks are an affront to the political sovereignty or territorial integrity. If this determination of just cause is affirmative, then an option to use physical force could be on the table. While fulfilling these two criteria does not alleviate the responsibilities of the rest of Just War Theory, they present an excellent perspective for analyzing a proper response.

Endnotes

[1] Tom Gjelten, "Pentagon Strategy Prepares for War in Cyberspace," *NPR,* http://www.npr.org/2011/07/15/137928048/u-s-military-unveils-cyberspace-strategy (accessed March 2, 2016).

[2] MG Paul Nakasone, "Cyber Domain," Theater Strategy and Campaigning Lesson 10-L (Carlisle Barracks, PA: U.S. Army War College, December 10, 2015).

[3] U.S. Army Maneuver Center of Excellence, "Maneuver Leaders Self Study Program: Nature and Character of War and Warfare," http://www.benning.army.mil/mssp/Nature%20and%20Character/ (accessed March 2, 2016).

[4] "Cyber" is so commonly misused that it is called out in Joint Publication 1-02, Figure B-3, as one of the most commonly misused terms in joint warfare.

U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), B5.

[5] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* Joint Publication 3-12 (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013), GL4.

[6] Interestingly, DoD Joint Publications use the term "domain" regularly but never define the term. This definition is from the Merriam-Webster online dictionary and applies to most, if not all, uses of "domain" in the Joint Publications.

[7] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, II-1.

[8] Kyle Genaro Phillips, "Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain," *Joint Forces Quarterly* 70 (3rd Quarter 2013): 72-73.

[9] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, II-5.

[10] Michael N. Schmitt, gen ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013), 1.

[11] Ibid., 106.

[12] "Su Bin, Chinese Man Accused by FBI of Hacking, in Custody in B.C.," *CBC News*, July 12, 2014, http://www.cbc.ca/news/canada/british-columbia/su-bin-chinese-man-accused-by-fbi-of-hacking-in-custody-in-b-c-1.2705169 (accessed March 2, 2016).

[13] While Saints Augustine and Thomas Aquinas writings that became Classic JWT predate the Westphalian conception of states, they treated war as an activity between princes. These wars were more personality driven, but the analogy between pre-Westphalian princes and States is generally considered to hold across the ages.

[14] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, II-5.

[15] Stanford Encyclopedia of Philosophy, "War," July 28, 2005, http://plato.stanford.edu/archives/fall2008/entries/war/ (accessed March 2, 2016)

[16] Ibid.

[17] George R. Lucas, Jr. and Rick Rubel, eds., *Ethics for the Military Professional: The Moral Foundations of Leadership,* 4th ed. (Boston, MA: Pearson Learning Solutions, 2011), 232-233.

[18] R. Craig Nation, "History, Theory, War, and Strategy," lecture, U.S. Army War College, Carlisle Barracks, September 9, 2015, cited with permission of Dr. Nation.

[19] For the purposes of clarity in this research project, any political entity will be referred to as a "state." In the complex world of asymmetric warfare, many groups claim to be legitimate governments, but they are rarely attacked from outside (and when they are, the outside agents are typically asked to intervene by the ruling government, such as Russia's involvement in the 2015 Syrian Civil War), making civil wars or insurgencies internal questions. For more about Legitimate Authority, see Stanford Encyclopedia of Philosophy, "War."

[20] Institute for Advanced Study, "Michael Walzer," https://www.ias.edu/people/faculty-and-emeriti/walzer (accessed December 18, 2016).

[21] Lucas and Rubel, *Ethics for the Military Professional*, 232.

[22] Stanford Encyclopedia of Philosophy, "War."

[23] Jeff McMahan, "Just Cause for War," *Ethics & International Affairs* 19, no. 3 (Fall 2005): 1, http://www.philosophy.rutgers.edu/joomlatools-files/docman-files/Just_Cause_for_War.pdf (accessed March 2, 2016).

[24] U.N. Charter, chapter 7, art 51.

Chapter seven of the U.N. Charter allows for warfare in the case of international agreement through the UN, but absent that international agreement, self-defense is the only permissible cause for war.

The First Gulf War in 1991 is an excellent demonstration of collective self defense: Iraq invaded neighboring Kuwait, and the expulsion of Saddam Hussein's forces was an international effort sanctioned by the United Nations Security Council and led by the United States.

[25] Michael Walzer, *Just and Unjust Wars,* 5th ed. (New York: Basic Books, 2015), 62.

[26] Ibid., 63.

[27] Ibid., xiv.

[28] Walzer specifically refers to "armies and insurgents" as modern war, but it seems fair to extrapolate his commentary to all forms of asymmetric warfare.

[29] Walzer, *Just and Unjust Wars,* xiv.

[30] Ibid., 51.

[31] Ibid., 58.

[32] Ibid., 61-63.

[33] Ibid., 58, 51.

[34] Ibid., 51.

[35] John Westlake, *Collected Papers,* ed. L. Oppenheim (Cambridge, England: 1914), 78, quoted in Walzer, *Just and Unjust Wars,* 53.

[36] John Locke, *The Works of John Locke: A New Edition*, ed Rod Hay (London, England: McMaster University Archive of the History of Economic Thought, 1823), 107.

[37] Walzer, *Just and Unjust Wars,* 54.

[38] Ibid., 55.

[39] Many Just War theorists (although not all) consider a preemptive strike justifiable, although both sides will likely disagree in any specific case. In any circumstance, it would be very difficult to argue that a cyber attack is a justified preemptive attack unless it is *directly* preventing some form of aggression.

[40] Schmitt, Tallinn Manual, 45.

[41] Walzer, *Just and Unjust Wars,* 89.

[42] Alexander Moseley, "Just War," http://www.iep.utm.edu/justwar/ (accessed December 19, 2015).

[43] Oliver Laughland, "FBI Director Stand by Claim that North Korea was Source of Sony Cyber-Attack," *The Guardian Online,* January 7, 2015, http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey (accessed January 12, 2016).

[44] A Distributed Denial of Service, from Webopedia.com, is "DDoS is a type of DOS attack where multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. According to… eSecurityPlanet, in a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin." Vangie Beal, "DDoS Attack – Distributed Denial of Service," http://www.webopedia.com/TERM/D/DDoS_attack.html (accessed January 11, 2016).

[45] Joywang, "The 2007 Estonian Cyberattacks: New Frontiers in International Conflict," *On Cyber War-Freshman Seminar 43Z-Internet Law*, blog entry posted December 21, 2012, https://blogs.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/ (accessed January 11, 2016).

[46] Emily Cadei, "Iowa Caucuses Go High Tech," *Newsweek Online,* January 8, 2016, http://www.newsweek.com/iowa-caucuses-go-high-tech-412958 (accessed February 24th, 2016).; Mario Trujillo, "Nevada GOP to Report Caucus Results With Smartphones," *The Hill Online,* February 22, 2016, http://thehill.com/policy/technology/270257-nevada-gop-to-report-caucus-results-with-phone-and-pictures (accessed February 24th, 2016).

[47] Walzer, *Just and Unjust Wars,* 57.

[48] Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal* 54 (December 2012): 4, http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf (accessed December 19, 2015).

[49] The assumption here is that there is not a declared state of war. If in a declared state of war, then the use of violence is legal and even to be expected.

[50] Ryan Jenkins, "Is Stuxnet Physical? Does It Matter?" *Journal of Military Ethics* 12, no. 1 (2013): 72.

[51] Ibid., 72.

[52] Stanford Encyclopedia of Philosophy, “War.”

[53] Ibid.

[54] Walzer, *Just and Unjust Wars,* 84.