2018

THE FAILED APPLICATION OF JUST WAR DOCTRINE TO CYBERWARFARE

Dalton E. Runyon
Southern Illinois University Carbondale, drunyon20@siu.edu

THE FAILED APPLICATION OF JUST WAR DOCTRINE TO CYBERWARFARE

by

Dalton Runyon

B.A., Southern Illinois University, 2016

Submitted in Partial Fulfillment of the Requirements for
the Master of Arts

Department of Political Science
in the Graduate School
Southern Illinois University Carbondale
May 2018

RESEARCH PAPER APPROVAL

THE FAILED APPLICATION OF JUST WAR DOCTRINE TO CYBERWARFARE

By

Dalton Runyon

A Research Paper Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Arts

in the field of Political Science

Approved by:

Dr. Stephen Shulman, Chair

13 April 2018

Graduate School
Southern Illinois University Carbondale

AN ABSTRACT OF THE RESEARCH PAPER OF:

DALTON RUNYON, for the Master of Arts degree in POLITICAL SCIENCE, presented on APRIL 13, 2018, at Southern Illinois University Carbondale.

Title: THE FAILED APPLICATION OF JUST WAR DOCTRINE TO CYBERWARFARE

MAJOR PROFESSOR: Dr. Stephen Shulman

Just War Theory has not followed with the most recent evolution of warfare. The last iteration of Just War Theory was created by Michael Walzer following the evolution of the tools of war in World War II. The current status of *jus ad bellum* and *jus in bello* are only applicable to conventional warfare, as this paper will show. Many current problems exist when attempting to analyze cyber attacks including the necessity of a proper definition, the determination of use of force, and how cyber attacks can be addressed in the future. These problems must be addressed so states can properly decide on how to make policies in relation to cyber attacks.

TABLE OF CONTENTS

HEADING 1

INTRODUCTION

Since the turn of the 20th century, technologies and the military industrial complex have been rapidly advancing. As technology advances, so does the desire and ability to weaponize it or use it militarily. Two of the most critical advancements are the invention of the computer and the internet. These two technologies have revolutionized the world in everyday life so that individuals and countries have become dependent on these systems and networks. This dependency creates a new realm of warfare for these countries but also creates an equal weakness to this realm of warfare, including an impact on the when, where, what, why, and how information is stored, transported, acquired, stolen, etc. The ability to wreak havoc or steal information from the other side of the world has revolutionized warfare making it much harder to prevent, stop, or determine who has caused these attacks. The significant advantage to anonymity is an unfortunate benefit to cyber attacks. The world has become very small, while simultaneously allowing actors to stay farther away from one another.

This new realm of warfare has produced a problem within the theoretical framework of international relations: the thought process behind the ethics and legality of warfare has not advanced alongside the technology. Although conventional warfare itself is always evolving, cyber advancements have led to a new type of espionage and warfare that is very difficult to define, and continues to blur the lines between what is conventional warfare and what is not. Can cyberwarfare follow the same guidelines as conventional warfare? Since technology is not static, cyberwarfare will be harder to define without a new set of criteria established now. These lines will continue to be blurred as technology advances and will be even harder to define if there is no set definition of cyberwarfare. Once a base definition is established for cyberwarfare, the issue of

applying ethics and determining how to evaluate cyberwarfare must be addressed. This paper will argue that the evolution of just war has not followed the evolution of conventional warfare, and must evolve to include these considerations so states can respond to these attacks.

The concept of a just war dates back millennia to Ancient Egypt, but the first iteration of the concept commonly referred to today as Just War Theory is rooted in Christian ideology. The first two main contributors were St. Augustine and St. Thomas Aquinas. St. Thomas Aquinas laid down the most basic concepts of a just war before the invention of the first modern gun, let alone the invention of electricity, missiles, or nuclear weapons, and yet the concept remained essentially unchanged until it was most recently advanced by Michael Walzer in his response to the Vietnam War.

In his advancement of the theory, Walzer stayed within the Christian philosophy, but he evolved the theory to fit the technological changes of that time period. Walzer did not drastically change the theory as the basic concepts of self-defense, and last resort can still be a possibility regardless of the technological advancements of conventional warfare. However, the era of Just War Theory as the sole doctrine has come to an end. Having guidelines for a just war is necessary, but as the doctrine stands now it is not capable of providing guidelines for cyberwarfare. These concepts presented in Just War Theory cannot be translated into the world of cyberwarfare. A proper analysis of Just War Theory through the lens of cyberwarfare is necessary to explain the downfalls of the application because even states are using the existing framework when analyzing cyber attacks. For example, the United States' Department of Defense, in an open report to the United States' Congress, stated: "If directed by the President, DoD will conduct offensive cyber operation consistent with the policy principles and legal

regimes that the Department follows for kinetic capabilities, including law of armed conflict."[1] These applications fail to accurately analyze a cyber attack, and cannot continue to be used in this manner. Just War Theory must evolve to be able to properly analyze cyber attacks, so that states can, if necessary, properly commit cyber attack.

In this paper, I will discuss the failures of application of the doctrine of Just War Theory to cyber attacks and cyberwarfare. However, before the analysis of Just War Theory's application to cyberwarfare, creation of a proper definition of cyberwarfare is necessary. Too many different definitions make it difficult to understand how to apply ethics or legality to this type of warfare. Following the definition, I will examine the existing approaches for determining if a cyber attack is considered a use of force. It is imperative to determine use of force before analyzing Just War Theory because it determines how a state can or should respond to an attack. Knowing how a cyber attack can be equated to a conventional attack determines how a response to cyber attacks can occur. Next, I will move into analysis of Just War Theory's application through *jus ad bellum* and *jus in bello*. After this I will move onto if and how preemptive and preventive attacks can be used as or in response to a cyber attack.

A note should be made that through this paper there will be an inclusion of some legal frameworks and some determinations later on based on legality. Just War Theory is an ethical doctrine and the results of this paper will argue for a continued ethical approach to determine if Just War Theory can be applied to cyberwarfare, but these legal frameworks are important to consider. These frameworks explain the thought process behind the doctrines created in relation to warfare. This paper will use these considerations to use legal frameworks to guide future ethical frameworks.

---

[1] United States Department of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, 5 (Nov. 2011)

Before a proper definition can be created, there must be an understanding of the different types of attacks that can happen in the cyber realm. One must understand different types to be able to create a definition that includes all types. Too many definitions, as this paper will later discuss, fail to be inclusive of all categories. To do this I will separate attacks into three different categories: propaganda, sabotage, and espionage. An actual cyber attack may fall across the boundaries of more than one of these categories, but these three categories best represent the different areas of cyberwarfare.

Conventional espionage as defined by *Merriam-Webster* is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company."[2] This holds true in the cyber realm, except cyber espionage is much easier for anyone to engage in. States, non-state actors, and individuals can all participate in cyber espionage. However, whether it is acquiring information or providing information, cyber espionage is very similar to traditional espionage.

Cyber propaganda includes the dissemination or alteration of data in the cyber realm to affect the opinions or information received by individuals. This can happen through either the changing of information on a website or through the spread of false information on forums or social media. The most extreme versions of cyber propaganda can be easily equated to psychological warfare, just occurring in the cyber realm.

Sabotage, the final category of cyberwarfare includes many types of attacks and holds many of the questions of how to apply ethics to cyberwarfare. Examples of sabotage can include simple distributed denial of service (DDoS) attacks, as well as complete sabotage of the utilities services of a country. This category contains the most physically destructive and harmful attacks.

---

[2] Dictionary by Merriam-Webster: America's most-Trusted online dictionary." Merriam-Webster. https://www.merriam-webster.com.

The best example of a cyber weapon, the Stuxnet virus, is included in this category. Further discussion of the Stuxnet virus will be included throughout this paper. Viruses, worms, and malware all fall into this category.

Although these categories are not difficult to explain, it is necessary for the categories to be laid out. The definitions commonly used for cyberwarfare often are only inclusive of one of these categories. Example definitions will be laid out in the next category, but these categories help to explain the failures of these definitions.

HEADING 2

DEFINITION OF CYBERWARFARE

The problem defining what cyberwarfare is stems from the use of multiple terms used interchangeably, as well as each organization or article defining cyberwarfare as it fits their argument or view. For example, the Tallinn Manual defines cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[3] The international law experts who wrote the Tallinn Manual use a definition that correlates closely to that of conventional warfare, focusing on damage and bodily harm. It is easy to see that this relates to the term they are defining, cyber attack. However, this definition fails to include any aspect of cyber espionage or cyber propaganda. Along with these exclusions, the definition does not even fulfill the aspects of the sabotage category. A DDoS attack could occur without any physical damage or harm, but could cause major disruptions to a state. The Tallinn Manual's focuses on only an extreme aspect of cyberwarfare..

Another commonly cited definition comes from the United States' Department of Defense. The DoD defines "computer network attacks" as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[4] However this definition fails to include the very cyber weapon the United States was suspected in creating: the Stuxnet Virus. The virus was transferred from a USB drive to computers inside the nuclear facility. From there the virus found its way into the centrifuges in Iran, rendering the centrifuges useless, but it in no

[3] Schmitt, Michael N., and Luis Vihul. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge, United Kingdom: Cambridge University Press, 2017.
[4] United States of America. Department of Defense. Joint Terminology for Cyberspace Operations. By James E. Cartwright. Washington, DC, 2010.

way disrupting, denying, degrading, or destroying information existing in a computer or a computer network.

These two example definitions are too narrow, therefore, fail to encompass the entirety of cyberwarfare. Another aspect that needs to be considered when properly defining cyberwarfare is the distinction of computers and computer networks being the *instruments* or the *objects* of attacks.[5] The failure of the object based approach is illustrated by the DoD's definition: "Disrupt, deny, degrade, or destroy information resident in computers and computer networks." It is not uniquely possible to accomplish this via a cyber attack. The destruction of a computer or computer network could be accomplished by conventional warfare: guns, bombs, or EMPs could all accomplish this. So to properly distinguish cyberwarfare, one must include an instrument-based approach to the definition.

Along with this a computer or a computer network may not even be the object of attack. Again, the Stuxnet virus proves this position. The Stuxnet virus was designed to solely destroy the centrifuges in a specific type nuclear power facility. The virus accomplished its goal of causing the centrifuges to spin out of control irreversibly damage them, but this attack completely negates the possibility of an objects-based definition. The object of the attack was neither a computer nor a computer network. The virus was transferred via USB thumb drive into a computer and manipulated computer data to show normal spinning speeds, but that wasn't the object of the attack. Although the object was the centrifuges, the virus was created on a computer, requiring the need for an instrument-based definition to properly separate cyberwarfare from kinetic warfare.

[5] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 (August 1, 2013).

Reese Nguyen provides the best base definition of cyberwarfare, but it is not perfect: "A hostile act using a computer or related networks or systems to cause disruption or destruction for a political or national security objective."[6] This definition creates several distinctions that are beneficial to discussing Just War Theory and cyberwarfare. First, the distinction of being instrument-based is essential. As discussed, the computer as the instrument of the attack specifies separation from conventional warfare. The definition also leaves open the possibility of all types of attacks by using the phrase "cause disruption or destruction." It allows for the inclusion of all three categories of cyberwarfare: espionage, propaganda, and sabotage. The third and final distinction is the inclusion of the wording "political or national security objective." This separates cyber hacktivism and basic cybercrime from cyberwarfare. This is the main exclusionary principle of the definition, and it allows for the exclusion of basic cybercrime from cyberwarfare.

The main problem with Nguyen's definition relates back to the problem of blurred lines. One major instance of blurred lines between cyberwarfare and conventional warfare is that of strikes by drones and other remote-controlled weapons. These remote-controlled attacks arguably fall under this definition of cyberwarfare. A drone strike could be classified as a "hostile act using a computer or related networks or systems to cause disruption or destruction for a political or national security objective."[7] However it is difficult to deny the inclusion of remote-controlled weapons as a cyber attack. If a foreign entity were to hack the drone and take control of it, then as a national security issue would this not be considered a type of cyber attack that would fall into the category of sabotage?

---

[6] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 (August 1, 2013).
[7] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 (August 1, 2013).

Nguyen's second failure of his definition is that it fails to include any part of cyber espionage that would not cause disruption or damage. This must be included to have a succinct definition.

Similarly, one cannot deny that a cyber attack could end with the use or sabotage of conventional weapons. A foreign entity could attack a network controlling conventional weapons and could disrupt, destroy, or set off these weapons. Because of this, Nguyen's definition must be changed. Therefore, I propose an update of Nguyen's definition to include these considerations. A cyber attack is *a hostile act or espionage using a computer or related networks or systems to cause disruption or destruction for a political or national security objective, excluding the use of one's own computer-based remote-controlled conventional weapons*.

HEADING 3

DETERMINING USE OF FORCE

With a proper definition of a cyber attack, evaluation of the application of Just War Theory on cyberwarfare can take place. The focus will only be on *jus ad bellum* and *jus in bello*. The point of this evaluation is twofold: whether cyber attacks can be considered a use of force, and whether the applications of *jus ad bellum* and *jus in bello* can be used to properly determine the validity cyber attacks. Determining the use of force, as mentioned, is imperative because it helps understand how to evaluate a cyber attack. Knowing the severity of a cyber attack and how it can be related to a conventional attack helps to understand how current ethical doctrines can or cannot be applied to cyber attacks. Considerations must also be made for the fact that many types of cyber attacks have only been theorized, and actual examples are slim for analysis.

A broader analysis of *jus ad bellum* and *jus in bello* will occur later in the paper, but it is necessary to give a brief explanation to covet the importance of this section. *Jus ad bellum* is the criteria to determine whether going to war is just, and *jus in bello* is the criteria to determine if one's actions in war are just. Because cyber attacks are so inherently different from conventional attacks sometimes it is difficult to determine what is actually a use of force. Using a computer to sabotage is not the same things a dropping a bomb on another state, but is using that computer constitution a use of force? This section will explore that question.

To consider the application of *jus ad bellum* and *jus in bello*, one must determine if a cyber attack could ever be considered a use of force. International law defines use of force based on two different organizations: The United Nations and the International Court of Justice. Although Just War Theory is not legally binding like these definitions, they are important to note to understand the thinking of diplomats and militaries when determining potential attacks.

Ambiguities in the United Nation's Charter create problems in properly defining what use of force is while the ICJ with its persuasive legal authority has created a better definition through their decisions. It is important to understand what use of force is for two reasons. First one must determine if Just War Theory can properly be applied, and second, one must know if a state can ever respond to a cyber attack with armed force.

According to the United Nations Charter Article 2(4): "All members shall refrain in their international relations from the threat of use of force against the territorial or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[8] Although prohibiting the use of force, the article does not explicitly define what a use of force is. As Nguyen explains, it is possible to infer what the drafters of the Charter meant for a use of force to be by examining other portions of the document.

One such section to determine the drafters' intent is found in Article 42, in which the Security Council, is allowed to use some conventional measures: "demonstrations, blockade, and other operations by air, sea, or land forces."[9] Nguyen also cites the mission of the United Nations found in the preamble of the Charter, "to ensure that armed force shall not be used, save in the common interest."[10] Thus, according to Nguyen, the minimum for a use of force is what occurred in the First and Second World Wars, and is what is discussed in these sections. Along with this, the United Nations has not challenged the use of economic or political coercion as uses of force, and as a collective, the international community has accepted that a use of force does not include "spaced-based surveillance, boycotts, and espionage."[11] These excerpts from the charter and

---

[8] UN Charter art. 2 para. 4
[9] UN Charter art 42 in Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4, p 1113 (August 1, 2013).
[10] UN Charter preamble in Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1114 (August 1, 2013).
[11] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1114 (August 1, 2013).

views from the U.N. give a framework as to what can be classified as a use of force as it is currently understood.

Also, to understand use of force, one must also understand when an attack is or is not in self-defense. The ICJ has played a major role in determining when self-defense is allowed in relation to determining what a use of force is. On one hand, Ryan Patterson in his article *Silencing the Call to Arms* points out that the ICJ, commenting on United Nations Charter Articles 2(4) and 51, "recognizes the inherent rights of self-defense against armed attacks, apply to 'any use of force, regardless of the weapons employed.'"[12] On the other hand, Nguyen points out that the ICJ ruled that arming and training guerilla warriors was considered a use of force but merely funding them did not. But even then, the ICJ failed to define what the use of force or armed attack is.[13]

The use of force and armed attacks have been inferred from two major world structures, the U.N. and the ICJ. The U.N. does not explicitly define the use of force, but through the inference of other sections of the charter, the use of force pertains solely to conventional warfare and excludes espionage. The ICJ through legal proceedings has touched on both use of force and armed attack. The ICJ interpretation of self-defense from the U.N. charter uses the terms, "armed attack" and "weapon." It must be determined whether a cyber attack ever reached the level of use of force it would also have to answer the question of is it an armed attack and in turn, answer the question of if a state can invoke its right of self-defense. These are important determinations because of the principle of last resort in *jus ad bellum*. States can only go to war after all other considerations are made, unless it is an act of self-defense.

---

[12] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244, 39 (July 8). 108. Advisory Juri in silencing the call to arms

[13] Military and Paramilitary activities in and Against Nicaragua (Nicar. V. U.S.), 1986 ICJ. 14, 199-120(June27)

HEADING 4

EVALUATING USE OF FORCE

Attempting to find direct parallels between cyber attacks and conventional warfare is a difficult task due the vastly different methods of both. As discussed in the definition section, even when the end goals are the same, the methods are not straightforward. Standard definitions of use of force fail to properly analyze cyber attacks. For example, a computer virus could render part of a state's military capabilities useless, which would have the same effect as launching an air strike, but with no physical invasion or human casualties. On the other hand, Nguyen also points out that a DDoS attack could cause economic harm by interrupting a victim state's trading capabilities with all states, not just with the perpetrating state attacking as sanctions do.[14] Clear debates have arisen to determine how to classify a cyber attack as a use of force or not. The next sections will discuss different approaches to attempt to work through the ambiguity of determining whether a cyber attack could be considered a use of force or an armed attack. After the discussion of these approaches, I will analyze the principles of *jus ad bellum* and *jus in bello*.

Can a cyber attack ever reach the same potential level of use of force of conventional warfare? This question is essential to determine if Just War Theory can be applied to cyberwarfare. The difficulty to answer this question stems from the fact that cyber attacks include a wide-range of methods to commit the attacks. Certain methods for cyber attacks could fall into the category of use of force or an armed attack and other methods may not. Some individuals argue that human casualties or destruction of critical infrastructure of the state must exist in order for a cyber attack to be considered a use of force while others consider any type of intrusion to constitute as a use of force dependent upon what is being attacked. To work around

[14] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1116 (August 1, 2013).

this issue, a system of categories similar to those used for the creation of the definition of cyberwarfare must be used to properly examine different methods for determining what constitutes the use of force. The types of cyber attacks are again broken down into three categories: instrument-based, target-based, and effects-based approaches.

HEADING 5

INSTRUMENT-BASED APPROACH

The instrument-based approach considers the tool used to commit the attack to determine if the weapon has physical characteristics that are associated with conventional military attacks.[15] The origins of this approach stem from a textualist reading of the articles of the United Nations Charter discussed above. Although the definitions of use of force and armed attack are not provided in articles 2(4) and 51 of the Charter, the inferences discussed earlier from the capabilities of the Security Council coupled with statements from the U.N. Resolution on the Definition of Aggression confirm that these terms relate solely to conventional military warfare.[16] Although the definition of aggression from the resolution leaves the possibility of cyber attacks being included, the examples given of what aggression can be excludes a possibility of a cyber attack being considered a form of aggression. The definition of aggression from the resolution is as follows: "Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition."[17] Per the definition set forth by the resolution, an argument could be made that cyber attacks could be considered an armed attack, if the resolution had not created set examples of what it determines to be the only forms of aggression. The examples set forth by the resolution collectively focus on invasions, territory violations and blockades through use of conventional warfare, completely excluding cyber attacks from being included in any possible use of aggression.

---

[15] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1117 (August 1, 2013).
[16] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1117 (August 1, 2013).
[17] General Assembly resolution 3314, *Definition of Aggression,* A/RES/3314 (14 December 1974).

Based on this textualist reading of United Nations documents, the instrument-based approach focuses only on the initial method of the attack, not on the consequences of an attack. Nguyen uses the example of a naval blockade against a state versus a trade embargo against a state.[18] The consequences or results of both situations could end up as identical, but the methods of attack are completely different. The difference in methods is all that matters to the instrument-based approach. The naval blockade is considered illegal under the United Nations' definition of aggression, but the trade embargo is not considered illegal. Although there is a difference between physical and diplomatic means being exerted, the overall approach cannot be used to determine if a cyber attack is considered a use of force. This approach limits itself too much and does not include new forms of warfare. Nguyen provides two examples in which this situation is illustrated. The first is the possibility of an information embargo. An information embargo could occur if one state has superior networking and intelligence capabilities that could block another state's intelligence capabilities. This attack could cause a state to become isolated but without a physical use of force that would violate the definition of aggression mentioned above. The second example is the Stuxnet virus. As mentioned previously, this virus was used to disrupt the functions of the Iranian nuclear facility. An identical outcome could have happened through the use of an air attack or missile, but because an air attack or missile was not used, this attack is not considered a use of force by this category.[19] Similarly major attacks against military capabilities or utility grids could have serious negative effects but would not fall into the instrument-based category because of the textualist reading. The incapability of this textualist approach and the difficulty to be able to adapt to different types of warfare proves the instrument-based approach

[18] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1118 (August 1, 2013).
[19] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1119 (August 1, 2013).

is a poor way to determine if these cyber attacks can be considered a use of force or armed attack.

HEADING 6

TARGET-BASED APPROACH

This approach is straight forward: the use of force or armed attack is based on the target of an attack. Proponents of this approach believe that any cyber attack against a critical infrastructure, such as utility grids, should be considered an armed attack.[20] Similar to the instrument-based approach, the target-based approach is very easily applied, but there are two major issues.

The first issue is that critical infrastructure is not a generally defined term that could be easily applied to all states. For example, the United States' Congress has defined its own critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, rational economic security, national public health or safety, or any combination of those matters."[21] Russia, on the other hand, defines critical infrastructure much differently. The Russian government determines critically important objects through three criteria. The first criterion determines the type of threat, whether it is against economic, military or socially significant targets. The second criterion is the scale of the catastrophe. It is a six point scale based on the human, material and spatial impacts. The scale's six points are local, municipal, territorial, regional, federal, and trans-border. The last criterion is the importance of the object in terms of three spheres: impact of the object on the regional economy, possible damage caused to state prestige, and threats to population and territory.[22] Even China has a different view on

[20] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1119 (August 1, 2013).
[21] Critical Infrastructure Protection Act of 2001,42 U.S.C. § 5195c(e) (2006)
[22] Pynnöniemi, Katri. Russian critical infrastructures Vulnerabilities and policies. Helsinki: Ulkopoliittinen instituutti, 2012.

critical infrastructure as outlined in a document focused specifically on critical information infrastructure and its cyber-defense policies.[23] Although overlap exists amongst states' own policies, there is no set overarching definition of critical infrastructure making this approach difficult to use.

The second issue is that the target-based approach itself is too broad. The nature of this approach only considers any level of intrusion on the target an armed attack. Although any cyber intrusion may be considered illegal this, does not necessarily justify an armed response. Because of the nature of these attacks, proponents believe that conventional, anticipatory self-defense strikes in response to cyber intrusions are viable. Because of this claim some scholars have stated that legally allowing these self-defense strikes would have strong deterrent effects. This claim is difficult to believe due to the internationally accepted practice of state-sponsored cyber espionage.[24] States do not expect there to be a conventional warfare response to these cyber intrusions.

Collectively these problems in the target-based approach, create more issues as well. For example, the United States has sixteen critical infrastructure sectors as defined by the White House. These sectors are so inclusive that seemingly any cyber intrusion "other than those targeting an individual's personal computer would permit responsive force" regardless of the nature of the intrusion.[25] Malware as small as datamining or the 2007 DDoS of Estonia would be considered intrusions allowing for a conventional response under these circumstances. Due to the lack of a set definition of critical infrastructures and the all-inclusive nature of the target-based

---

[23] Trioli, Paul, Rogier Creemers, and Graham Webster. "China's Ambitious Rules to Secure 'Critical Information Infrastructure'." New America. July 14, 2017. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/.
[24] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1119 (August 1, 2013).
[25] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1121 (August 1, 2013).

approach, this approach falls short of being able to properly examine if a cyber attack qualifies as a use of force.

HEADING 7

EFFECTS-BASED APPROACH

This approach focuses on the effects and results of an attack. This approach does not disregard the target or instrument used for the attack but does not weigh these two categories as importantly as the results of the attack. Additionally, an important separation is delineated between conventional and cyberwarfare. In conventional warfare, a strong correlation exists between intent, cause, and effect.[26] Cyber attacks, on the other hand, are unpredictable and could have repercussions that would not be foreseen. The attacks could also repeatedly fail with no effect.

The most prominent examination of the effects-based approach for determining if a cyber attack is considered a use of force is a method laid out by Michael Schmitt.[27] Schmitt created an analysis based on six criteria, but even these criteria have inherent faults. The criteria are:

1. Severity--the degree of physical injury or property damage.
2. Immediacy—how quickly the negative consequences manifest
3. Directness—the proximity of the act and its consequences
4. Invasiveness—the extent of territorial penetration
5. Measurability—to what extent the consequences can be quantified
6. Presumptive legitimacy—whether the ac is presumed valid under domestic or international law.[28]

---

[26] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1122 (August 1, 2013).
[27] Nguyen, Reese. "Navigating Jus ad Bellum in the Age of Cyber Warfare." California Law Review, 4th ser., 101, no. 4 p 1122 (August 1, 2013).
[28] Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L. 885,914-15 (1999).

Although these criteria are efficient, they do not properly determine if a cyber attack can be considered a use of force. Schmitt himself applies these criteria to the 2007 Estonian DDoS attacks, finding that five of the six factors were in favor of the attack being a use of force.[29] However, Nguyen, in his own analysis, easily molds the criteria to find that the DDoS attacks do not constitute a use of force. The malleability of these criteria make this approach difficult because they can be interpreted in many different ways.

The *Tallinn Manual* also uses the effects-based approach, but even its analytical tools do not properly determine if a cyber attack is a use of force, as they concede that "the law is unclear as to the precise point at which the extent of death, injury damage, destruction, or suffering caused by a cyber operations fails to qualify as an armed attack."[30] It is also important to note that the *Tallinn Manual* authors point out that no international cyber incidents have occurred in which states have argued that these attacks have reached a use of force[31], which directly contradicts Schmitt's application of his criteria.

Another issue with the effects-based approach is the different capabilities of the target state. Dependent upon the target state's capabilities, the results of an attack could be entirely different than the exact same attack on a different state. Obviously, the failure of not just one approach but all three approaches requires a new approach to determine if a cyber attack could ever be a justified use of force."

---

[29] Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L. 885,914-15 (1999).
[30] Schmitt, Michael N., and Liis Vihul. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge, United Kingdom: Cambridge University Press, 2017 P. 55.
[31] Schmitt, Michael N., and Liis Vihul. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge, United Kingdom: Cambridge University Press, 2017 P. 56.

HEADING 8

WORKING TOWARDS A NEW APPROACH

The failure of these three approaches illustrates the difficulty of applying the current legal framework and the current doctrine of Just War theory to cyberwarfare. Without the proper tools of analysis to determine if a cyber attack is considered a use of force, one cannot full apply this doctrine. I would argue, however, that a single approach cannot fully analyze a cyber attack. The unpredictability of cyber attacks and the lack of definitions of related terms in the cyber realm that exist across all three approaches show that a new approach must encompass the benefits of multiple approaches while simultaneously removing the weakness of each approach. The only feasible approach that is capable of analyzing a cyber attack's use of force is a tripartite approach involving the three previously discussed approaches. This tripartite approach analysis of the target, the instrument, and the effects used is necessary. A focus too much on one or the other would fail the analysis. This tripartite approach allows for proper analysis without the downfalls of the individual approaches. Along with this tripartite approach, each attack must be considered on a case-by-case situation. Although all three approaches are necessary for proper evaluation of an attack and if it qualifies as a use of force, these three approaches individually prove that a single overarching precedent cannot be created to ethically determine if a cyber attack can be considered a use of force. Now that the determination of how a cyber attack can be considered a use of force, the evaluation of just war theory can occur.

HEADING 9

JUS AD BELLUM

In this section, I will analyze each principle of *jus ad bellum*, defining each one and explaining how that principle it can or cannot be applied to a cyber attack. The principles are as follows: just cause, just peace, legitimate authority, proportionality, and last resort.[32]

When committing an attack, a country must answer the question of just cause. It is the overarching principle of *jus ad bellum*.[33] Determining if a country has just cause is extremely important because the question is essentially determining if the death and destruction that results from the attacks is justifiable. It must be a thoughtful consideration to prevent offensive attacks just for national interest. For example: Is it a humanitarian intervention?; Does it reestablish peace?; Is it self-defense?; Or is it simply an attack committed for national interest? Walzer makes another key argument for this principle: the entanglement of sovereignty and territorial integrity. In the fourth edition of Walzer's *Just and Unjust Wars*, he introduces the argument of sovereignty into the section of just cause. The argument is rooted in the social contract that human rights and sovereignty go hand-in-hand. The contract exists because a state is responsible for the safety of its citizens, but in a humanitarian intervention, often the state is committing the crime and the intervening state must overrule this state's sovereignty. The problem of sovereignty will be discussed shortly.

One can easily decide if the reason for committing an attack is just or not, but the complete answer is not this easy. The Stuxnet attack, for example, destroyed another state's nuclear capabilities that had not weaponized, but it was believed that Iran planned on

[32] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).
[33] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).

weaponizing the uranium. Does this justify the use of Stuxnet? And does this justify Iran to respond with a use of force? One could argue that the Stuxnet Virus fulfills the principle of last resort for Just War Theory when considering a conventional attack, to be just, but the attack was not truly in self-defense and was certainly not a humanitarian intervention. Hypothetically if Iran were actively producing uranium to make nuclear weapons and had made active threats, then would Stuxnet be justified? I believe the answer per Just War Theory is still unanswerable. Although theoretical cyber attacks that have been discussed, could cause mayhem and do considerable damage like a conventional attack, I think it will always be used before a conventional attack because of the safety it offers to the state that is committing the attack. This point can be better seen in the next point made on sovereignty

Walzer, as stated, mentions sovereignty in his discussion, which is another complicated subject when transferring to the cyber realm. Traditional sovereignty or territorial integrity has been straightforward: a state controls what is inside its borders as determined by treaties, legal claims to land, etc. But these are all tangible, physical borders; what of the internet? Can a state enter another state's *digital borders*? If these so-called digital borders exist, how do they factor into just cause? States have varying degrees of privacy laws or internet blocks for their own citizens, as well. Stephen Krasner, in his book *Sovereignty: Organized Hypocrisy*, breaks sovereignty into multiple categories. Although written in 1999, it could be revised to include another category, digital sovereignty. His argument maintains though that only legal sovereignty and Westphalian sovereignty is necessary to the state,[34] so likely infringements on digital sovereignty would still raise many questions. The issue of whether or not a cyber attack can

[34] Krasner, Stephen D. Sovereignty Organized Hypocrisy. Princeton: Princeton University Press, 2001.

infringe on a state's sovereignty creates questions that cannot be answered by this traditional Just War Theory doctrine.

The second principle of *jus ad bellum* is just peace.[35] The concept of just peace is that a reasonable plan must be put in place to maintain the state after the war is over. One cannot plan to go into a state, decimate, and leave it. This principle is an extremely foreign concept to a cyber attack. Although a cyber attack may not be able to completely decimate a state, the extent of an attack cannot be easily planned as a conventional attack could. The Stuxnet virus escaped into the real world through an unplanned human action, even though it was never supposed to leave the nuclear facility. With the numerous unknown circumstances and the unpredictable consequences, it is not possible to use just peace

The third principle of jus ad bellum is legitimate authority. The principle of legitimate authority has a major problem with application to a cyber attack or cyberwarfare. Legitimate authority requires states to have the proper individuals declare a war.[36] It also takes away the ability for non-state actors to declare a war. Therefore two aspects to legitimate authority exist: war can only be declared by a recognized state, and war can only be declared by the proper individuals inside the recognized state.

China is regularly accused of state-sponsored cyber attacks on the United States, but it is difficult to prove and the power of denial makes legitimate authority difficult. Similar to state-sponsored terrorism, a state can sanction individuals or groups to commit cyber attacks, whether DDoS attacks or stealing information or any other number of attacks; the government can simply deny it even if it had given the legitimate authority. It is much more difficult to prove that these

[35] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).
[36] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).

individuals acted under the sanctioning of the government and therefore makes the overall aspect of legitimate authority difficult to prove. This in turn makes it difficult for the victim state to properly respond through Just War Theory. Without knowing the true assailants, a state could fail the criteria to go commit an attack.

To state more straightforwardly, the individual who has the legitimate authority to declare an attack or war would not change, but the ability for states to commit attacks and deny any involvement makes the concept of legitimate authority in the cyber realm convoluted. The ensuing response of a state could be misled or improper because of the difficulty of determining the legitimate authority.

The fourth principle of *jus ad bellum* is proportionality. Proportionality in *jus ad bellum* states that for a response to occur the reasons for must outweigh the reasons against going to war.[37] This principle does seem likely to easily be transferred to the cyber realm, unlike the other principles, however, to do this the new approach to determining use of force from above must be used. Once a state determines the effects and a severity of a cyber attack it can determine whether its response is proportionate or not.

The final principle of *jus ad bellum* is last resort. Last resort is simple: has every other possibility been considered and attempted to prevent the threat before an attack?[38] Once again, straightforward this is simple, but it is highly unlikely that a conventional attack would ever be considered before a cyber attack; more than likely it would be the opposite. A state would likely look to commit a cyber attack before a conventional attack to save the lives of its own citizens, if it is possible. Sometimes the reason for a cyber attack cannot be accomplished by a conventional

[37] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).
[38] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).

attack or vice versa. And yet, sometimes a cyber attack makes the end goal of a conventional attack easier to attain. The DDoS attack in Estonia was much easier to accomplish via cyber attack than some sort of EMP strike or conventional attack to stop internet usage. Since cyber attacks are not considered as serious as a troop invasion, and therefore last resort is much more difficult to consider for the cyber realm. While these attacks have the same end goal, the cyber attack may attain that goal with much less destruction, but that does not mean a cyber attack is any different from a conventional attack. The basic reasoning behind last resort is the same: all diplomatic possibilities, such as diplomatic talks or sanctions, have been exhausted. Cyber attacks continue to blur the line between what is and what is not considered the last possible option.

These principles of *jus ad bellum* collectively fail when applied to cyber attacks and cyberwarfare. The lines that have been blurred by cyber attacks have also created an impossible situation for applying *jus ad bellum* to cyberwarfare. The next section will focus on the application of jus in bello principles to cyber attacks and cyberwarfare.

HEADING 10

JUS IN BELLO

In this section, I will analyze each of the principles of *jus in bello,* defining each one and explaining how it relates to a cyber attack and whether it can or cannot be applied. The three principles of *jus in bello* are: discrimination, proportionality, and necessity.[39] The three principles in *jus in bello* are intertwined and incorporated with one another, as will be seen in the following discussion.

The first principle that will be discussed is discrimination. Discrimination prohibits the intentional targeting of noncombatants, unless the deaths are deemed comparable to the end goal.[40] The main consideration of discrimination is the individual right to life and liberty. Cyber attacks make this difficult to consider. Although a large majority of these attacks would pass this aspect on the sole reason that a majority of attacks are not deadly, certain attacks could still cause death or large scale human suffering dependent upon the target or scale of the attack. However, cyber attacks do bring up two key issues in this section that are more difficult to consider: who is a combatant in cyberwarfare and how can a cyber attack discriminate solely against targeting noncombatants.

Determining combatants in cyberspace is difficult because states do not have standing armies of cyber warriors. Individual cyber warriors could be in many different locations and different departments of a government or could be just contracted by the government. The United States' DoD stated in a report to Congress that "the Department has the capability to

[39] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).
[40] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).

conduct offensive operations in cyberspace to defend out Nations, Allies and interests."[41] The DoD's statement shows that a state may have dedicated cyber warriors but does not address specifically who these individuals are nor where they work from, just that they were employed by the DoD. Along with this issue is the problem of anonymity. Although the individuals responding to a cyber attack should be highly skilled and could determine the origin of a cyber attack, it may take some time, they could make some mistakes, and, as a result, the wrong individual or group could be targeted in a response. It should be noted, however, that as long as the intent to target the correct individuals is there it would be considered ethical.

Sean Watts in his article, *The Notion of Combatancy in Cyber Warfare* attempts to answer this question of combatancy, but also concludes that in its current framework, the legal system also cannot determine combatants from noncombatants. He uses four criteria from the 1874 Brussels Declaration to determine the legal framework of combatants.[42] The four criteria from the declaration to determine combatants are:

1. That they be commanded by a person responsible for his subordinates;
2. That they have a fixed distinctive emblem recognizable at a distance;
3. That they carry arms openly;
4. That they conduct their operations in accordance with the laws and customs of war.[43]

Watts explains that although the declaration never attained legal status, the criteria were used in doctrines for the next 100 years until 1977, when the Geneva Convention was altered, and even then, these criteria heavily influenced that writing.[44] Watts is skeptical of a blanket application of

---

[41] United States Department of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, 5 (Nov. 2011)
[42] Sean Watts the notion of combatancy in cyber warfare
[43] Project of an International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874.
[44] Watts, Sean. "The Notion of Combatancy in Cyber Warfare." SSRN Electronic Journal, 2012. doi:10.2139/ssrn.2484823.

these criteria onto the cyber realm. Watts only mentions retention of the first criterion. Although it is only a "formalistic and empty requirement," in the cyberspace realm, this criterion allows for the exclusion of individual actors.[45] The next two criteria can be extremely difficult to apply in the cyber realm. Both criteria make it possible for clear distinction of who the combatants are, but cyber attacks speak to the element of anonymity. And with a direct interpretation of the third criterion, anyone with a computer could be a combatant. The fourth criterion should be a must, to ensure cyber warfare is held to the proper standards. This section proves that not only is it difficult to determine combatants in the cyber realm, but the ability to solely target combatants, if determined, is also very. Although this is a legal framework, unlike the ethical framework of Just War Theory, I believe it is an important discussion to be had because of the potentially massive differences between conventional warfare and cyber warfare. Changes in the thought process of warfare must change , and this framework is one that must be evaluated when moving forward to determine the ethics of cyberwarfare.

Even if a clear distinction of combatants could be made, being able to solely target combatants can be difficult. As stated before, if combatants are affected and the attack is comparable to the end result it is acceptable. However, Stuxnet provides an example of how more individuals or systems could be affected than intended, and potentially more than what is acceptable. The Stuxnet virus made it out of the nuclear facility and made its way into several states before being discovered. The virus was even being updated and controlled during the time it affect the nuclear facility.[46] Even with this degree of control, the perpetrators were unable to

[45] Watts, Sean. "The Notion of Combatancy in Cyber Warfare." SSRN Electronic Journal, 2012. doi:10.2139/ssrn.2484823.

[46] Watts, Sean. "The Notion of Combatancy in Cyber Warfare." SSRN Electronic Journal, 2012. doi:10.2139/ssrn.2484823.

keep a single variable, one worker at the nuclear facility, from spreading the virus to the outside world. The Stuxnet virus demonstrates that discrimination can occur in planning but cannot be controlled once the attack has left the solitary control of the perpetrator; as a result, discrimination, as it is currently defined, cannot be applied to cyber attacks. In conventional warfare it is typically easy to determine a civilian target from a military target, but cyber space is a realm inhabited by both civilians and the military.[47] This is not to say however that there are zero noncombatant deaths in conventional warfare, but that the unintended consequences of cyber attacks are not known as well as those in conventional warfare. Considerable changes must be made to move away from such stringent criteria that are related to armed attacks, so that the criteria can include cyber attacks.

The second principle of *jus in bello* is proportionality. Proportionality is similar to discrimination but broader when it comes to noncombatants.[48] To meet the criteria of proportionality, the harming of noncombatants must be proportionate to the end goals of the attack. The arguments in the previous discussion of discrimination about the distinction between combatants and noncombatants can be applied to proportionality with one important additionality consideration: the very different outcomes of conventional warfare and cyberwarfare.

Although cyber attacks could be wide-ranging and fatal, if this happens, it would most likely be through indirect measures, whereas, conventional warfare very directly causes human fatalities. Along similar lines, many cyber attacks do not have permanent, or long-lasting

[47] Moore, Stephen . "Cyber Attacks and the Beginnings of an International Cyber Treaty." North Carolina Journal of International Law 39, no. 1 p. 239 (2013)
[48] Lazar, Seth. 2016. “War.” Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).

consequences.[49] A DDoS attack only causes disruptions during the attack, with potentially no consequences after the attack. However, in conventional warfare an air strike could have very long-lasting consequences. Therefore, the analysis of its proportionality would be of a very different nature than analysis of a conventional attack.

How a cyber attack will affect noncombatants is difficult to predict, even if it is closely controlled. I believe proportionality is necessary, just like discrimination for consideration in a legal evaluation of a cyber attack, but as Just War Theory currently stands, it cannot be applied.

Also, this principle is also difficult to relate to the cyber realm. Straight forward it seems easy, but after consideration becomes every complex. For example, the DDoS of Estonia in 2007 disrupted access to many government websites, banks, and news stations, but what is considered proportionate in response? Would a proportionate attack in response be a DDoS affecting the same number of websites? The same types of websites? Is the proportionate response to affect the same number of individuals? Is any response even allowed? It is hard to quantify these types of attacks.

What if the state is two times smaller? Even more difficult, what if Iran retaliated for the destruction of its nuclear facility? Would proportionality be one nuclear facility for one nuclear facility? But what if the significance of the nuclear facility that Iran chooses to retaliate is more important to innocent civilians? What if the facilities are different in size, capacity, or purpose? Although these questions are also difficult to answer in conventional warfare, the type of response is much more clear. The earlier determinants of whether a cyber attack is a use of force must be considered when determining proportionality. These criteria discussed previously help to determine a proportionate response that may not be as simple to determine as with conventional

[49] Moore, Stephen . "Cyber Attacks and the Beginnings of an International Cyber Treaty." North Carolina Journal of International Law 39, no. 1 p. 240 (2013).

warfare. Just War Theory, as it now stands, cannot be applied to cyber attacks because the what ifs overwhelm the concept of proportionality.

The third and final principle of *jus in bello* is necessity: the collateral harming of noncombatants is acceptable when the least harmful means of military attack are chosen to attain the goal.[50] This principle should be applied, overly aggressive or destructive cyber attacks are not necessary especially if noncombatants are overly affected by them. Again the Stuxnet virus speaks to the difficulty to do this. The possibility of an attack expanding further than planned, creates extreme difficulties for avoiding the targeting of noncombatants. Although this principle should be applied, it is once again, extremely difficult as it currently stands.

Overall, the aspects of *jus in bello* are difficult to apply to cyber attacks. The main problems stem from the inability to determine combatants from noncombatants and the issue of proportionality and necessity are difficult to directly translate from application of an armed attack to application of a cyber attack.

[50] Lazar, Seth. 2016. "War." Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/war/ (February 16, 2018).

HEADING 11

PREEMPTIVE AND PREVENTIVE STRIKES

Two additional aspects of Just War Theory, which aren't direct principles of *jus ad bellum* and *jus in bello,* deserve consideration for cyber attacks: preemptive strikes and preventive strikes. Both preemptive and preventive strike are considered anticipatory, first strike, defensive measures.[51] Preemptive strikes are generally viewed as allowable under Just War Theory; whereas, preventive attacks are typically viewed as unjust.[52] Israel provides an example of each of these. Israel's strike on Egypt that started the Six Day War in 1967, illustrates a preemptive strike. The verbal interactions between the Egyptians and Israelis over ownership of part of the Sinai Peninsula had escalated and in June 1967, the Egyptians mobilized their troops on the border of Israel. Before the Egyptians could strike, on June 5th, 1967, the Israelis launched a preemptive strike on the Egyptians and their allies, pushing them back and resulting in a signed ceasefire only six days later.

While this strike is perceived as a just, preemptive strike in self-defense, the Israelis also have a clear-cut case of an unjust, preventive attack.[53] Preventive attacks are similar to preemptive attacks in that the state attacking views it as a first strike in self-defense, but the difference is the threat is not as immediate as that in a preemptive attack. In 1976 Iraq purchased a French nuclear facility called Osirak claiming only peaceful intentions for the facility The Israelis, however, believed that the Iraqis were planning on weaponizing the material produced by the facility. Due to this suspicion, the Israelis launch an air strike on June 7th, 1981, which

---

[51] Barnes, Joe, and Richard J. Stoll. 2007. "Preemptive and Preventive War: A Preliminary Taxonomy." THE JAMES A. BAKER III INSTITUTE FOR PUBLIC POLICY RICE UNIVERSITY.
[52] Barnes, Joe, and Richard J. Stoll. 2007. "Preemptive and Preventive War: A Preliminary Taxonomy." THE JAMES A. BAKER III INSTITUTE FOR PUBLIC POLICY RICE UNIVERSITY.
[53] Barnes, Joe, and Richard J. Stoll. 2007. "Preemptive and Preventive War: A Preliminary Taxonomy." THE JAMES A. BAKER III INSTITUTE FOR PUBLIC POLICY RICE UNIVERSITY.

destroy the facility. The attack was illegal. Even if the Iraqis planned on weaponizing the material, they were years from accomplishing this, so there was no immediate threat.

Are these types of attacks possible in the cyber realm? I believe that answer to be yes. The separation between immediate and non-immediate threats must continue to be applied even when analyzing cyber attacks; however, just like every other aspect of cyberwarfare thus described, an inapplicable grey area exists. In a hypothetical situation, State A has threatened a missile strike on State B; the threat and attack seem viable, so it would be preemptive and therefore legal for State B to commit a cyber attack to take out these missiles. If, however, State B commits a cyber attack to destroy these missiles solely based on the belief that State A has missiles that could possibly be used in a future attack with no immediate threat, the cyber attack would be preventive and therefore illegal.

These are important points to consider due to the combined statements of the United Nations charter and ICJ suggesting inherent right to self-defense. The United Nations Charter Articles 2(4) and 51, "recognizes the inherent right of self-defense against armed attacks, […] to 'any use of force, regardless of the weapons employed.'"[54] Although previously determined in this paper that these articles cannot be applied to cyber attacks, the issues that arise for self-defense must be considered. Other doctrines defend and attack the possibility of preemptive strikes. The Bush doctrine is one such recent doctrine that defends the use of preemptive strikes. Following the terrorist attacks of September 11th, 2001, the United States moved into the Middle East and embedded itself into the regions' affairs. This movement into the Middle East included in 2003 a so-called preemptive strike on Iraq due to evidence that Saddam Hussein had WMDs. Although the actual legality of the attack has be4n questioned since new evidence came to light,

[54] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244, ¶ 39 (July 8). 108. Advisory Juri in silencing the call to arms

in 2003 this doctrine raised several valuable points for the argument in favor of preemptive strikes. However, the Bush doctrine only appears to muddle the examination of cyber attacks. On the other hand, Kofi Annan, then Secretary-General of the United Nations, argued against any type of anticipatory self-defense in 2005.[55] Although I have argued in this paper that the United Nations' Charter clearly fails in the cyber realm Anna's arguments that preemptive strikes are not legal should be considered."

The issue, however, comes from the application of preemptive and preventive strikes in response to threats of cyber attacks. It is easy to determine the effects of a conventional attack but not as simple for cyber attacks. The main issue is how does a state know the full effects of a cyber attack. State A could threaten to topple State B's utility framework, but how does one judge these capabilities? How does State B know that their cyber defenses, already in place, cannot prevent these attacks? And, how does State B respond? Does State B respond by preemptively taking down State A's utility framework? Or would State B preempt with a conventional attack? Within preventive attacks this is extremely important because anonymity and distance for a cyber attack may prevent State B from knowing that State A is planning an attack, even if State B is completely aware of State A's capabilities. This situation would not even leave time for a preemptive attack or a preemptive attack. In a society where arguably every state has some level of cyber capabilities, it is hard to see preventive attacks ever being considered legal because it is extremely difficult to assess these capabilities, and the Bush doctrine creates even more difficulties for this. Although a state cannot just idly sit waiting for a fatal blow,[56] the capabilities of cyber attacks are always present, and an attack could happen at

[55] Kondoch, B. (2013). Jus ad Bellum and Cyber Warfare in Northeast Asia. Journal Of East Asia & International Law, 6(2), 459-478. doi:10.14330/jeail.2013.6.2.06
[56] Kondoch, B. (2013). Jus ad Bellum and Cyber Warfare in Northeast Asia. Journal Of East Asia & International Law, 6(2), 459-478. doi:10.14330/jeail.2013.6.2.06

any time. Further threats must occur to justify such an attack because there may not be noticeable mobilization that would be necessary to prepare for an attack similar to the Egyptian build up around Israel in 1967. The *Tallinn Manual* agrees with this sentiment, stating that a state may act in self-defense "when the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts."[57] The difficult part of this evaluation comes from determining if a cyber attack can equate to a use of force. In this case the results portion of the tripartite evaluation would have to be skipped due to the immediacy for the threats.

Overall, these arguments point to a continued failure of legality to allow for preventive attacks, but a preemptive cyber attack appears viable for both a conventional and a cyber threat. Although no precedent exists and the full power of a state's cyber capabilities may not be known, the ability to use an anticipatory self-defense strike when validly threatened seems to be a legal response. The level of response, however, would be based on the threat and the known capabilities of the other state.

[57] Schmitt, Michael N., and Liis Vihul. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge, United Kingdom: Cambridge University Press, 2017.

HEADING 12

MOVING BEYOND JUST WAR THEORY

With the failure of application of *jus ad bellum* and *jus in bello*, the question is how does a state respond to a cyber attack? Even in cases, such as preemptive strikes, when extenuating circumstances would justify the use of a cyber attack, grey areas exist. As this paper has shown the ability to apply Just War Theory and similar aspects of conventional warfare to the cyber realm is not possible. Suggestions to remedy this situation also fall flat. A few of these suggestions are presented by Marco Roscini in his article *World Wide Warfare-Jus ad bellum and the Use of Cyber Force*. He presents three resolutions to this problem: resort to the United Nations Security Council, resort to an international court, and retortions and countermeasures.[58]

The argument for resorting to the Security Council is embedded in Article 35 of the United Nations Charter: "Any Member of the United Nations may bring any dispute, or any situation of the nature referred to in Article 34, to the attention of the Security Council or of the General Assembly."[59] (Article 34 states: "The Security Council may investigate any dispute, or any situation which might lead to international friction or give rise to a dispute, in order to determine whether the continuance of the dispute or situation is likely to endanger the maintenance of international peace and security.")[60] Although this solution is a sound diplomatic and legal solution, one must consider the permanent members of the Security Council. The United States, China, and Russia, three of the largest perpetrators of cyber attacks, hold veto power in the Security Council. Although an attack may not stem from these three states, they could veto an any action against themselves, or against an ally.

---

[58] Roscini, Marco. "World Wide Warfare - Jus ad bellum and the Use of Cyber Force." Yearbook of United Nations Law 14, no. 2010 (2010).
[59] United Nations Charter Art. 35 para. 1
[60] United Nations Charter Art. 34

The second solution provided, resorting to an international court, has its own inherent issues as well. Roscini mentions the possibilities of a victim state requesting an international tribunal or an advisory opinion of the ICJ to determine the legality of a cyber attack, but this method would only be viable if there is no further immediate threat.[61] If these attacks lead to a conflict or if the attacks are severe, the victim state may not have the time to wait for a tribunal or the ICJ to determine the legality. Also, the perpetrating state may not be a signatory of an international court. The United States is not a member of the International Criminal Court and therefore could not be prosecuted or held responsible to rulings of this court.

Roscini's last answer to this dilemma, retortions and countermeasures, is too broad and faulty in logic. His argument that the attack would have to be deemed illegal is true., but because cyber espionage is considered legal through state practice, a state could not deem this type of intrusion as illegal.[62] However, he continues to cite the United Nations Charter, which, as discussed, fails to properly determine if a cyber attack can be considered a use of force. Countermeasures are important, but not a solution to the problem.

Another possibility would be a new international treaty in relation to the use of cyber warfare. The major downfall of a treaty is that a state would have to become a signatory to be held to its principles, but the norms created could become widely accepted. Even if not universally signed, the creation of a widely accepted treaty could force permanent members of the Security Council to act accordingly.

Similar to norms being accepted, the treaty could create definitions for use of force and armed attack that could be widely used correcting issues that currently exist in the realm of cyber

[61] Roscini, Marco. "World Wide Warfare - Jus ad bellum and the Use of Cyber Force." Yearbook of United Nations Law 14, no. 2010 (2010).
[62] Roscini, Marco. "World Wide Warfare - Jus ad bellum and the Use of Cyber Force." Yearbook of United Nations Law 14, no. 2010 (2010).

warfare. A universal acceptance of norms and definitions is needed for the legal framework to be updated in relation to cyber warfare, either through an international treaty or the creation of a cyber Just War Theory. Along with the determination of these definitions and norms, the ability to determine who perpetrated a cyber attack is extremely important. As discussed, the issue of anonymity is prevalent throughout cyber warfare, but if a treaty could properly outline the evidence needed to determine fault, whether state or nonstate actor, then creating legal consequences becomes much easier to outline and enforce.[63]

[63] Moore, Stephen . "Cyber Attacks and the Beginnings of an International Cyber Treaty." North Carolina Journal of International Law 39, no. 1 p. 242 (2013).

HEADING 13

CONCLUSION

The evolution of ethical norms regarding conventional warfare have failed to be applicable inside the realm of cyberwarfare at the most basic of levels. The creation of a proper definition was necessary before beginning any analysis of current doctrines. Previous definitions focused on too specific of concepts or excluded different types of cyber attacks to define cyberwarfare. These definitions often only focused on a target or instrument-based approach, but by applying the effects-based approach and stating the exclusion of computer-controlled conventional weapons, a proper definition was created.

Once this definition was created, one more step was necessary to perform the examination of the relationship of Just War Theory and cyber warfare. This next step was to determine if a cyber attack can ever reach the level if a use of force or armed attack. Traditional analysis and international doctrines that cite use of force and armed attacks, fail in the cyber realm. The wide-ranging types of cyber attacks and the lack of exact definitions in doctrines for use of force and armed attack create problems for this application. The United Nations Charter has proven to be incapable of evaluating if a cyber attack is considered a use of force. The instrument-based, target-based, and effects-based approaches all have inherent benefits and failures, but individually fail to determine if a cyber attack can be considered a use of force. To properly analyze if a cyber attack can be considered a use of force, a tripartite analysis of the categories must occur on a case-by-case nature. The target, the instrument used, and the results must all be considered.

After creating a proper method to determine if a cyber attack can be considered a use of force, analysis of both *jus ad bellum* and *jus in bello* occurred. The analysis of each individual

principle showed that the attempts to apply these standards of conventional warfare prove futile when applying the standards to the cyber realm. The blurred lines that cyber warfare create cause too many issues for a simple translation of the current Just War Theory from conventional warfare to cyber warfare.

Along the lines of Just War Theory arose the question: could cyber attacks be used in anticipatory self-defense strike. The basic applications of preventive and preemptive strikes appear to translate well to cyberwarfare. Preventive attacks in the cyber realm are illegal, just like in conventional warfare, but a preemptive strike could be possible if the proper criteria are met. The argument for a cyber preemptive strike against a threatened cyber attack is harder to make than a preemptive strike if threatened with a conventional strike, but both seem legal and viable.

To remedy these issues, others have attempted to find solutions to move forward or to show how a state could currently act in response to a cyber attack, but these solutions also fail. The bias of states and the lack of a governing body that would hold states to international court proceedings prove these methods nearly impossible to be fairly applied. Although the same could be said about the creation of an international treaty, this solution is the best way to move forward to address the cyber realm. If an international treaty can be created that properly defines and analyzes the aspects of Just War Theory and that can be nearly universally accepted, the norms and definitions will exist for proper determinations. Since Just War Theory is used to create norms for legal doctrines, and since it does not properly address cyber attacks, this document must be updated so states can properly this new realm of warfare in their policies.

VITA

Graduate School
Southern Illinois University

Dalton Runyon

Drunyon20@gmail.com

Southern Illinois University Carbondale
Bachelor of Arts, Political Science May 2016

Research Paper Title:
The Failed Application of Just War Doctrine to Cyberwarfare

Major Professor: Dr. Stephen Shulman