DISTRIBUTION AGREEMENT

In presenting this thesis as a partial fulfillment of the requirements for a degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis in whole or in part in all forms of media, now or hereafter know, including display on the World Wide Web. I understand that I may select some access restrictions as part of the online submission of this thesis. I retain all ownership rights to the copyright of the thesis. I also retain the right to use in future works (such as articles or books) all or part of this thesis.

Ishaan Jalan December 18, 2013

Cyberwarfare: Military Ethics and the Applicability of Just War Theory

By

Ishaan Jalan

Dr. Nicholas Fotion

Advisor

Emory University Department of Philosophy

COMMITTEE

Dr. Nicholas Fotion

Emory University Department of Philosophy

Dr. Noëlle McAfee

Emory University Department of Philosophy

Dr. Benn Konsynski

Goizueta Business School | Halle Institute for Global Learning

December 20, 2013

ACKNOWLEDGEMENTS

I cannot express the gratitude I have for my committee for their continued support and encouragement: Dr. Nicholas Fotion, my advisor and committee chair; Dr. Noelle McAfee and Dr. Benn Konsynski, my committee members. I am deeply indebted to you for the learning and guidance you afforded me during my time at Emory.

This project could not have been completed without the support of my friends – Nikhil, thank you for spending countless hours reading and re-reading my thesis to check for objectivity, grammar, etc. – it is most appreciated. Also, thanks to my academic advisor, Valerie Molyneaux, for supporting me in all my endeavors and taking the time to attend my defense.

Finally, to all the unnamed people who supported me through this entire process: thank you. Your generosity will not go unnoticed.

Cyberwarfare: Military Ethics and the Applicability of Just War Theory

By

Ishaan Jalan

Dr. Nicholas Fotion
Advisor
Emory University Department of Philosophy

An abstract of
a thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Business Administration with Honors

Department of Philosophy

2013

ABSTRACT

Cyberwarfare: Military Ethics and the Applicability of Just War Theory

By

Ishaan Jalan

This thesis seeks to determine if ancient ethical traditions in military ethics such as Just War Theory can be applicable to modern-day scenarios involving cyberwarfare. The first chapter discusses the development of weapons over time, starting with conventional, chemical and nuclear weapons and how the proliferation of cyberweapons will be exponentially faster than the proliferation of other types of weapons in the past. The second chapter introduces the various tenets of Just War Theory as well as some of the criticisms leveled against it in the past and currently with regard to its applicability to cyberwarfare. The third, fourth, and fifth chapters present three modern-day cases involving cyberwarfare and the application of the Just War doctrine to determine if 'cyber-aggression' or 'cyber-attacks' can be justified or not. I conclude that despite many claims that Just War Theory is outdated, it can be successfully applied to conflict situations involving cyberweapons and any suggestions that it is obsolete as an ethical theory are misguided. While there may be a time in the future when cyberwarfare takes on a persona that is so far removed from its current state that Just War Theory is no longer applicable, it does not appear that this will be the case in the near future.

Cyberwarfare: Military Ethics and the Applicability of Just War Theory

By

Ishaan Jalan

Dr. Nicholas Fotion
Advisor
Emory University Department of Philosophy

A thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Business Administration with Honors

Department of Philosophy

2013

TABLE OF CONTENTS

INTRODUCTION

In order to consider the ethics of cyberwarfare within the broader spectrum of military ethics, it is imperative we understand how cyberwarfare fits into the modern political theatre. Conventionally, we refer to anything that has the ability to harm or destroy a person or physical entity as a weapon. Over time, we have seen what commonly constituted a 'weapon' change as humans developed better and more sophisticated instruments of war. During World War I and World War II we saw great use of weaponry that is now described as "conventional" – referring to bombs, guns, etc. that could be used to kill or maim directly. The World Wars also saw the gradual development of chemical weapons i.e. nerve agents packaged in the shell of conventional bombs that caused widespread death across a large unspecified target area. The Manhattan Project and deployment of the first atomic bomb over Hiroshima forever changed modern weaponry and played a big part in nuclear weapons becoming a means of deterrence as seen during the Cold War between the United States and Soviet Union. All these developments had one thing in common: they involved weapons that had a direct measurable impact that could be traced to the infliction of harm to human lives and the damage or destruction of physical objects. However, the rapid development of the Internet and the cyberspace after the Cold War has placed such a narrow definition of "weapon" into doubt. The broad classification of weapons as they exist today (with examples) is as follows:

a. Conventional Weapons: guns, rockets, knifes, swords, etc. are all considered conventional weapons. These are typically the most common types of weapons used by the army, navy, and air force.
b. Chemical Weapons: mustard gas, sarin gas, RX, and other chemical compounds that are lethal in nature. Such weapons are prohibited under the Hague Convention although this

rule has been violated over the course of World War I and II as well in recent cases involving oppressive regimes suppressing civilian rebellions.

c. Nuclear Weapons: Usually an explosive device that uses nuclear fission or a combination of nuclear fission and fusion to release large quantities of energy in a destructive manner. The first use of a nuclear weapon was the United States' atomic bombing of the cities of Hiroshima and Nagasaki in 1945.

What constitutes a Cyberweapon?

Cyberwarfare is unique from any of the weapon classifications mentioned above. It is suggested that cyberweapons constitute the first new major form of weapons since the advent of nuclear weapons in the second World War. As Randall Dipert notes, "the acknowledgement of attacks that have been coordinated by the central commands of governments (or other political organizations) and that are directed at another country's governmental and military information systems" is quite new.[1] There are several distinctions between cyberweapons and other types of weapons (conventional, chemical, and nuclear):

a. Physical Nature: While conventional, chemical, and nuclear weapons are tangible in some form, cyberweapons are not physical in nature – they comprise of computer 'bugs' or 'viruses', code that can be used to infect other computers and systems that are a major component of military infrastructure today. This makes it very easy for any state to acquire cyberweapons, as they are created based on the knowledge of a subset of computer programmers colloquially known as 'hackers' and not nuclear materials such as plutonium, uranium, etc. as is the case with nuclear weapons. As a result, the

[1] Dipert, Randall R.: "The Ethics of Cyberwarfare." Page 385. Journal of Military Ethics Volume 9, No. 4. Published by Routledge in 2010.

proliferation of cyberweapons has bee considerably faster than the proliferation of any other type of weapon over the course of the previous century.

b. Effect or Damage: While the use of most types of conventional, chemical, or nuclear weapons results in death and destruction, the use of cyberweapons may not be lethal or even cause physical damage to any object. This distinction afford users of cyberweapons to limit the degree of collateral damage[2] (or eliminate collateral damage entirely) that is difficult to control when states employ the other types of weapons available to them.

While cyberweapons have varying degrees of usage in cyberwarfare, they can also be used by individuals and non-military groups for the same intents and purposes as other types of weapons. As cyberwarfare is relatively new in itself, varying accounts classify cyberweapons as those used to spy on other nations and gather information as well as cause damage to systems and infrastructure. However, for the purpose of this paper, the use of cyberweapons for espionage or intelligence gathering is not discussed. Only a subset of cyberweapons is discussed because of several reasons. First, the large (and growing) number and types of cyberweapons would be impossible to discuss adequately and would serve no purpose with regard to this discussion. Second, cyberweapons are used by individuals and non-military/state organizations goes beyond the purview of Just War Theory and are often cases of cyberterrorism, hacking, etc. and not cyberwarfare. Third, Just War Theory is primarily used to judge the actions of recognized states and not terrorist groups (as such groups are not considered to abide by any ethical code) and thus, only cyberweapons used by states to conduct cyberwarfare against other states falls within the purview of this discussion.

[2] Damage or harm that is incidental to the intended target i.e. civilians killed in a strike against a military compound.

Cyberwarfare as the Weapon of Choice

The rapid militarization of most developed countries over the last century, spanning two World Wars and several regional conflicts, has forced military ethicists to reevaluate their philosophy with regard to international conflict. Cyberwarfare is increasingly becoming the weapon of choice for both legitimate governments and shadowy militant organizations around the world. The Central Intelligence Agency, Syrian Electronic Army, and the hacker group "Anonymous" are all examples of groups that have used the cyber sphere to further their goals. While such use is widespread, only the cyberweapons programs of the CIA, Mossad, and other government-backed organizations are discussed in cases going forward. Modern technology has irrevocably replaced many weapons of the past, the concept of the World Wide Web as a battlefield is only just being realized. Cyber-weapons have made it possible for a hacker[3] or anyone skilled in the art of extracting information, gaining access to secured servers[4] in order to manipulate its functions, etc. over the Internet to be able to cause chaos across continents with the click of a button.

The United States, a leader in the computing world and certainly one of the first sovereign states to widely adopt the World Wide Web, has maintained a powerful arsenal of cyber weapons for several years. This arsenal has allowed the U.S. to effectively contain threats from antagonistic countries such as Democratic People's Republic of Korea and the Islamic Republic of Iran. Due to the security and secrecy provided by these cyber weapons, the United States was able to perform clandestine operations against Iranian nuclear facilities, destabilizing their efforts to enrich uranium and other nuclear minerals for their nuclear program. However, this all changed in 2011 when an error in the programming code for the worm used by the U.S.

[3] A person who secretly gets access to a computer system in order to get information, cause damage, etc.
[4] A computer or computer program that manages access to a centralized resource or service in a network.

cyber weapons program against Iran revealed the bug to the rest of the world. This program, code-named “Olympic Games” was authorized under the presidency of George W. Bush and continued during the Obama administration. The increased scrutiny following this revelation, complemented with sensitive information released by Edward Snowden, has revealed to the world the increased scope and capabilities of the U.S cyberweapons program.

It is evident that any ethical theory within the realm of military ethics is going to have be applicable to cyberwarfare in order to stay relevant. In this paper, it is the intention to discuss how Just War Theory may be applicable to cyberwarfare and how its applicability demonstrates that the use of cyberweapons (while very different in nature from other types of weapons) may still be governed by the principles of the Just War doctrine.

IN DEFENSE OF JUST WAR THEORY

Several critics have argued that Just War Theory is hopelessly outdated and cannot be applicable to modern day war scenarios, especially those that involve cyberwarfare, robotic weaponry and situations that do not include the human element that was ever-present in conventional warfare. It may appear that Just War Theory, an ancient doctrine dictating the decision to go to war and the manner in which it must be fought, is not suitable with regard to assessing cyberwarfare. However, later in this paper we will attempt to address some of these criticisms by applying Just War Theory to assess the use of cyberwarfare in three modern-day scenarios involving the use of cyberwarfare. Before we go any further, it would be imperative for us to define the two parts of Just War Theory: *jus ad bellum* and *jus in bello*.

Jus ad bellum

The first part of Just War Theory, jus ad bellum, pertains to the justice of the war and literally translates to the "right to fight". It questions whether a nation is justified in going to war and provides six principles that a nation must satisfy in order to be considered just when engaging in conflict. The six principles of jus ad bellum, as defined in "War and Ethics: a new just war theory" by Nicholas Fotion, are as follows[5]:

a. Just Cause: The just cause principle of jus ad bellum identifies whether a nation has a good reason for entering into a state of war with another nation. The Just war doctrine identifies six reasons that are considered 'good enough' to satisfy the just cause principle. Three of the six reasons are related to the defense of one's own nation and the remaining three are related to the defense of others. Just cause is satisfied if a nation goes to war in self-defense – when it is under attack, when it has been recently attacked, and when it is

[5] Fotion, Nicholas: "War & Ethics: A New Just War Theory." Chapter 2: Just War Theory. Continuum International Publishing 2007.

about to be attacked in the near future. Furthermore, a nation also has just cause if it engages in war to defend others in similar circumstances, or when a genocide is taking place in another nation and the nation is in chaos. This is because Just War Theory believes that a nation may go to war on humanitarian grounds to alleviate the suffering of civilian populations facing the genocide, as the cost of such intervention would be lower than the cost of allowing the genocide to continue.

b. Last Resort: The last resort principle of jus ad bellum discusses how a nation must take appropriate steps to ensure that going to war is the last option for the nation after all other measures have failed. This is to prevent leaders from engaging in war without negotiating with the other side, imposing sanctions, and exhausting all manner of diplomatic options. The purpose of Just War Theory is not to encourage war by providing means for justification and the last resort principle is proof of this. However, it should be known that the last resort principle does not typically apply to nations that go to war in response to an attack, as negotiating with the attacking party is not likely to be successful.

c. Proportionality: The proportionality principle of jus ad bellum discusses the costs and benefits of going to war. For a war to be just, the expected benefits must significantly outweigh the costs of the war. If the costs of a war are expected to be greater than the estimated benefits, the proportionality principle will tell us that the nation should not go to war. This principle is often difficult to satisfy as estimating the costs and benefits of war can be inaccurate especially in the case of prolonged conflicts where the costs far exceed the estimates made at the onset of the war.

d. Likelihood of Success: The likelihood of success principle is similar to the principle of proportionality but is related to the outcome of the war as opposed to the costs and

benefits. The principle states that a nation must only go to war if it has a reasonable chance of winning the war or being successful in achieving its objectives. For example, the principle would prevent a nation from going to war that the nation was destined to lose irrespective of the reason. An issue with this principle is the notion of success and what success may be defined as. Since military conflicts have different objectives, varying types of success could be used to satisfy this principle in the context of war.

e. Right Intentions: The principle of right intentions is associated with the decision making of the aggressor in a war. The principle suggests that for a war to be just the nation that goes to war must have good intentions and is not going to war to profit territorially or to acquire another nation's resources. An example of a nation having the right intentions would be one that engages in war to stop genocide or defend an ally that has been attacked or is under attack. It is quite easy to determine what the intentions of a country were with the benefit of hindsight and hence the principle of right intentions has served as an important tool in determining if past wars were just or not.

f. Legitimate Authority: The principle of legitimate authority of jus ad bellum is related to the person(s) who have been given the authority by the people of a nation to decide whether to go to war or not. It states that war can only be authorized by a person with legitimate authority to do so and any war started by a person without such authority is unjust. It is usually not difficult to identify whether a person with legitimate authority started a war although the advent of the United Nations and other coalition bodies such as the North Atlantic Treaty Organization (NATO) has affected the debate surrounding legitimate authority. Scholars often argue whether legitimate authority still resides with the nation state or whether the U.N. and NATO override the authority of the nation state.

Jus in bello

The second part of Just War Theory, jus in bello, pertains to the justice in how a war is waged. In a sense, it provides guidelines on how a nation can be just while fighting a war. The two principles of jus in bello are as follows:

a. Proportionality: The proportionality principle of jus in bello is significantly different from the proportionality principle that is part of jus ad bellum. This principle is concerned not with the costs and benefits of a war, but rather the degree of force used in individual campaigns during the war. It states that a nation should not use excessive force when dealing with the enemy. An example of this would be using a nuclear bomb to level a fortified city that you are unable to capture. However, the principle of proportionality does allow for a nation to use overwhelming force if the use of such force would lead to saving lives. An example of such a situation may be one where an enemy surrenders when encountered with the overwhelming force as opposed to putting up a fierce resistance.

b. Discrimination: The principle of discrimination of jus in bello reflects one of the oldest rules pertaining to war, which is that a nation warring with another must distinguish between military and civilian targets and not harm civilians. Several laws including those concerning war crimes by the Geneva Convention are based on this principle. It is quite easy to determine if a nation satisfies or violates the discrimination principle within the context of war. The discrimination principle could also be used when determining the method of attack for an army in order to minimize the risk of collateral damage to civilians that are not legitimate targets in any military campaign.

Common Criticisms of Just War Theory

As stated above, Just War Theory consists of two parts: jus ad bellum and jus in bello that are used to determine the justice of the war and justice in the war. According Nicholas Fotion, jus ad bellum has weaknesses due to the looseness and ambiguity of some of the principles and this is evident particularly across the just cause, good (right) intentions, and likelihood of success principles.[6]

Let us first consider the just cause principle of the Just War Theory. The problem caused by looseness or plasticity is magnified by the change to make the principle more open-ended. In effect, one powerful reason or a 'cluster of reasons' may now be cited to satisfy the principle. This cluster of causes introduces a fair share of problems, one of which is regarding what reasons may be cited in the cluster and how one may weigh the reasons within it. An example of such a cluster of causes could be the arguments used to justify United States' war in Iraq. The U.S. invaded Iraq since it believed Iraq was developing weapons of mass destruction and humanitarian intervention was needed to protect the Iraqi people from the dictatorship of Saddam Hussein. None of these reasons alone would provide sufficient cause to go to war, but combined together these reasons justified the war in Iraq. However, since no guidelines are presented on which causes may be cited, any warmonger may abuse the principle by finding sufficient reasons to satisfy the just cause principle by this method and proclaim the propagation of war as just. Beyond the clustering causes part of the principle, the main six reasons are also loose enough to induce problems of their own. An example of this would be the changing nature of aggression by different parties, especially in light of the recent news of cyber attacks conducted by the United States against Iran. In the past, an attack on a military target would be a

[6] Fotion, Nicholas: "War & Ethics: A New Just War Theory." Chapter 3: Objections to Just War Theory. Continuum International Publishing 2007.

just cause for war but the nature of a cyber attack is not as easily defined. The problem lies in determining what can be defined as aggression and what cannot by a majority of people and this ambiguity can be exploited to justify war using the just cause principle. This problem is further exacerbated by the continuous advancement of technology, especially in the realm of cyberwarfare, which further challenges the attribution and recognition of aggression.

The good intentions principle, as a part of the jus ad bellum portion of Just War Theory, presents problems because of the difficulty in ascertaining the intentions of a state when it engages in war. As we know from the just cause principle, a cluster of reasons or intentions may be behind a nation's participation in war and determining whether these reasons are backed up by good intentions is difficult, if not impossible. Furthermore, intentions often change over time, especially as new information is brought to light. For example, in the war in Iraq where it was discovered that the Iraqis did not have any weapons of mass destruction, the continuation of the war was justified by the intention to liberate the oppressed people in Iraq. The problem lies in the subjective nature of intentions and how the intentions of the people involved in the war may not be aligned resulting in ambiguity. In order to sort through a cluster of causes, one would have to identify the strongest motivation behind the war and determine whether it is intentionally good or right. Yet again, a dishonorable person//dictator could take advantage of this principle by presenting persuasive and good intentions behind his or her actions but having a hidden agenda in reality. Hypothetically, Russia could invade some of the former-Soviet Republics by suggesting that they want to protect the interests of ethnic Russians living in those areas. However, in reality their goal could be to gain a strategic geopolitical advantage or access to valuable resources which would not satisfy the good or right intentions principle of jus ad bellum but there would be no way to ascertain their real intentions.

Finally, another major weakness with the jus ad bellum portion of Just War Theory concerns the likelihood of success principle. In most cases, when a state goes to war, it evidently believes in victory or strategic success. Problems arise due to the difference in the strategic goals of conflicting states and determining whether any measure of success can be achieved without the benefit of hindsight. Furthermore, due to the nature of war, success is usually predicated at the outset but very rarely celebrated at the outcome. Lack of information about most states' combative strength and growth of mechanized weapons systems have blurred the ability to make accurate predictions about the outcomes of war. This is clearly evident in the United States' prolonged "War on Terror" and the questionability of its success. Thus, the looseness across the principles of jus ad bellum presents major weaknesses in the usefulness of Just War Theory with respect to modern day war scenarios.

The jus in bello portion of Just War Theory introduces two principles that determine justice in the war. Similar to the problems faced by the principles that determine jus ad bellum, the looseness of the discrimination and proportionality principle result in major weaknesses in the jus in bello part of Just War Theory. An examination of some of these shortcomings is discussed below.

The discrimination principle in jus in bello determines whether a state is just in a war based upon its differentiation of military and civilian targets. A problem is the looseness that exists with how far the principle of discrimination may be stretched as a war is prolonged or becomes serious for a nation. This occurred with Britain in 1940 when Nazi Germany occupied most of Europe and was on the brink of invading England. For a situation such as this, the Rules of Engagement may allow nations to attack targets not permissible under normal circumstances. In the circumstance or fog of war, nations often violate the principle of discrimination due to its

looseness and ambiguous nature. Furthermore, the list given with respect to the principle of discrimination is not exhaustive and thus allows states' to exploit the principle and overweigh factors of proportionality in justifying any actions taken against non-legitimate targets.

Let us take the case of the German bombardment of the city of London during World War II, which was clearly in violation of the principle of discrimination. The Luftwaffe commander, Herman Goering wanted to crush British morale by reducing their capital to ruins. The Germans believed by doing so they could negotiate a treaty in their favor and swiftly conclude the Battle of Britain. This illustrates a time when the principle of discrimination was ignored largely due to the prolonged and serious nature of the war. The strategic benefits of the war are largely given greater weight than the ethical importance of adhering to the principle of discrimination. The United States' atomic bombing of the islands of Hiroshima and Nagasaki is another case of weaknesses of the principles in jus in bello. While the bombings led to the surrender of the Japanese Armed Forces, the cost to civilians is still evident today and serves as a reminder of the costs to innocent human life when the principle of discrimination is flouted.

The context of civil war with respect to the principle of discrimination is very interesting as it blurs the differentiation of legitimate and non-legitimate targets even further. When the dictator of Libya, Muammar Gaddafi, targeted and attacked areas with rebel camps, there were several thousand civilian casualties as a result of his actions. In cities such as Benghazi and Tripoli, Gaddafi's forces engaged in torture and murder of innocent civilians who had not taken up arms. Similarly, Bashar al-Assad, the President of Syria has denounced civilian populations fleeing Syria as terrorists, which under the discrimination principle gives him the right to use force against them. Thus, the looseness and ambiguity of the principle allows such characterizations and allows dictators to defend the actions of their regimes.

The proportionality principle of jus in bello also contains weaknesses that undermine the usefulness of Just War Theory. Here, we consider the proportionality of individual battles or campaigns as opposed to the proportionality of a war as discussed in jus ad bellum. Logically, the cost–to–benefit ratio of an individual campaign or battle is much easier to assess than that of an entire war. Thus, one would assume that the proportionality principle works well with respect to jus in bello, or at least better than in the context of jus ad bellum. We are not concerned with this however, but rather whether it is useful in predicting if a side will be better off or worse off when the battle or campaign is completed. Due to the unpredictable nature of battles and asymmetric information usually available, predications concerning benefits and costs will vary with the nature of battle commanders and therefore not provide an accurate measure with which to consider justice in the war. Furthermore, battles are often influenced by additional factors that commanders do not foresee such as was the case in the failed Bay of Pigs invasion by the United States where CIA-trained Cuban exiles failed to overthrow the government of Fidel Castro. In this case, the CIA did not expect the Cuban forces to be trained by Eastern Bloc nations to prevent such action that ultimately led to the unsuccessful conclusion of the attack.

Therefore, jus in bello provides a guideline on how to approach situations within war ethically but are largely ignored in the prolonged nature of wars. The weaknesses in jus in bello allow unscrupulous leaders to commit injustices within wars, which further undermines the usefulness of the jus in bello portion of Just War Theory.

Just War Theory and Cyberwarfare

As indicated above, Just War Theory has some criticisms that have led detractors such as Michael Walzer at the Institute for Advanced Study (IAS) in Princeton, New Jersey to question its usefulness over the years. However, it is important to note that those are not criticisms Just

War Theory has faced with respect to its applicability to cyberwarfare, rather some criticisms it has faced as an ethical theory during the course of its formal existence. A proponent of the Just War doctrine, Colonel James Cook at the United States Air Force Academy, notes that "analogously ambiguous cases have long existed in warfare without undercutting the JWT's (Just War Theory's) broad relevance."[7] An analysis of historical cases of warfare shows that while Just War Theory may be difficult to apply in certain cases, it remains a powerful ethical standard that can be applied to help states approach war and engage in conflict in a just manner.

The rise of cyberwarfare in recent years has prompted critics such as Randall Dipert of the State University of New York to suggest that the Just War doctrine may no longer be relevant in the world of cyberweapons: weapons that are unique and have several unusual features in comparison to conventional weapons. According to Dipert the first issue with applying Just War Theory to cyberwarfare is the principle of just cause. Just cause for war is typically considered to be an aggression or attack by an enemy. As per the United Nations, an armed attack in the only condition under which a nation may justifiably defend itself before the Security Council takes action (UN Charter 1945: Ch. 7, Article 51). Dipert uses this definition to state that only an attack involving the use 'arms' that cause the infliction of death, injury, or physical destruction of objects may be considered as an aggression or attack[8]. He disputes W. Owens consideration of a cyberattack being a straightforward instance of an armed attack by suggesting that the effects of a cyberattack are not as obvious as those of bombs that led to the immediate deaths of soldiers in Pearl Harbor in 1941. However, with the benefit of hindsight, the claim that cyberweapons do not cause physical harm or damage to objects is easily discredited. As mentioned later in the case

[7] Cook, James: " 'Cyberation' and Just War Doctrine: A Response to Randall Dipert." Page 411. Journal of Military Ethics Volume 9, No. 4. Published by Routledge in 2010.
[8] Dipert, Randall R.: "The Ethics of Cyberwarfare." Page 395–396. Journal of Military Ethics Volume 9, No. 4. Published by Routledge in 2010.

study regarding the U.S. sponsored cyberweapons program against Iran, the Stuxnet virus used by the U.S. "produced physical damage of the Iranian nuclear facility comparable to that caused by the 1981 and 2007 Israeli air strikes that destroyed partially constructed nuclear reactors in Baghdad and Syria."[9] Furthermore, in the information age, military infrastructure is increasingly reliant on systems that are the targets of cyberattacks. Not only can cyberattacks destabilize the communications and operating ability of an army, but they can also cause weapons systems under the control of a virus to self-destruct and inflict death and injury to those in the vicinity of such systems. Dipert's analysis of cyberwarfare does not consider the sophistication of modern cyberweapons and the precision with which nations such as the U.S. are able to deploy them to achieve operational objectives through the destruction of enemy military targets.

As Colonel Cook states, "all of these existing and potential problems in the application of JWT (Just War Theory) to CW (Cyberwarfare) represent differences in degree, rather than kind."[10] It is clear that cyberwarfare presents some unique challenges to the application of Just War Theory due to its rather unique and unusual characteristics. In the following chapters, Just War Theory is applied to determine the just nature of cyberattacks in three recent scenarios involving the Islamic Republic of Iran, the Syrian Arab Republic, and the Democratic People's Republic of Korea. Each case presents different challenges to the application of the Just War doctrine and it is demonstrated that while applicability may be difficult, it is not impossible.

[9] Nguyen, Reese: "Navigating Jus Ad Bellum in the Age of Cyber Warfare." Page 1082. California Law Review, Volume 101: 1079. Published in 2013.
[10] Cook, James: " 'Cyberation' and Just War Doctrine: A Response to Randall Dipert." Page 422. Journal of Military Ethics Volume 9, No. 4. Published by Routledge in 2010.

CASE STUDY: IRAN

The application of Just War Theory requires a thorough understanding of the background of the conflict or aggression being assessed. In order to adequately discuss the United States cyberweapons program against Iran, it is important to delve into the background of Iran and United States relations. This is important from the perspective of understanding the reasons behind Iran being a primary target of several U.S. cyberweapons programs and whether such actions by the United States were justified. Furthermore, an examination of Iran's military arsenal is important with regard to assessing the threat Iran poses to the United States and its allies such as the State of Israel.

Relations between Iran and the United States

The United States' tenuous relationship with Iran ignited in 1953 when the Central Intelligence Agency orchestrated a coup replacing the democratically elected Prime Minister with the Shah of Iran, Mohammad Pahlavi. The Shah, however, was seen as a puppet of the United States. The Iranian Revolution was a direct response to U.S. influence and the coup it supported, as exemplified by the Iran hostage crisis in which 52 American diplomats were held hostage for 444 days. Relations declined further when the U.S. supported Iraq's invasion of Iran and hindered Iran's efforts to obtain international financial institution loans to fund its war efforts. Relations improved under the Clinton administration, but then in 2002, President George W. Bush publicly labeled Iran, along with North Korea and Iraq, as part of the "Axis of Evil"[11].

Furthermore, Iran has declared open hostility toward Israel, the United States' closest ally in the Middle East. In 2006, Ahmadinejad stated that the Holocaust is a myth and that he wants to

[11] Shoamanesh, Sam: "History Brief: Timeline of US-Iran Relations Until the Obama Administration". MIT International Review: Retrieved September 10th, 2013. <http://web.mit.edu/mitir/2009/online/us-iran-2.pdf>

see Israel "wiped off the map"[12]. Iran has thus far indirectly attacked Israel by supporting Hezbollah, the U.S.-classified terrorist organization based in Lebanon. Hezbollah and Iran share the view that Israel is an enemy of Islam. Thereafter, Hezbollah engaged in terrorist attacks such as suicide bombings and kidnappings. This alliance between Hezbollah and Iran has been of great concern to the US since Iran "has provided hundreds of millions of dollars in support of Hezbollah and has trained thousands of Hezbollah fighters at camps in Iran"[13]. With Hezbollah's political rise in Lebanon, its threat to Israel has increased substantially over the past several years. Such threats constitute a grave danger to American lives, both on the ground in the Middle East and in the form of terrorist strikes on American soil.

Iran's military and nuclear capability

In order to evaluate Iran as a threat to American lives, we must consider Iran's military prowess and nuclear capabilities. The Islamic Revolution Guard Corps (IRCG) was also created following the Iranian Revolution, which was the starting point for the antagonistic relationship between Iran and the United States. The IRGC has held considerable power in Iran since its creation and has expanded its military capacity independently of the national military and beyond its original mandate: "to protect the revolution and support revolutionary movements abroad, including those in Afghanistan, Iraq and Lebanon"[14]. The IRGC has 130,000 members within its five armed branches and commands the navy, air force, ground forces and the

---

[12] Siddique, Haroon: "Explainer: Relations between Iran and Israel." The Guardian on 25th September 2008. Retrieved September 10th 2013.
<http://www.guardian.co.uk/world/2008/sep/25/iran.israelandthepalestinians>

[13] Katzman, Kenneth: Iran: U.S. Concerns and Policy Responses. Congressional Research Service on 5th September 2012. Page 51, Retrieved September 9th 2013.
<http://www.fas.org/sgp/crs/mideast/RL32048.pdf>

[14] Salemi, Vahid. "Islamic Revolutionary Guards Corps (Quds Force)." New York Times on 3rd Oct. 2012. Retrieved September 12th, 2013.
<http://topics.nytimes.com/top/reference/timestopics/organizations/i/islamic_revolutionary_guard_corps/index.html>

intelligence service. Additionally, the IRGC has oversight over Iran's missiles, nuclear program, and its multibillion-dollar business empire. Furthermore, the Quds Force, a special operations unit under the IRGC, is involved with a number of international military and suspected terrorist activities such as the training and arming of Hezbollah in Lebanon and Shiite militias in Iraq. Another prominent division of the IRGC is the Basij militia; a citizen paramilitary force tasked with containing protests and dissidents[15].

Iran has a history of military conflict and, as a result, the country has invested in its naval capabilities to protect interests in the Persian Gulf. Following the First Persian Gulf War (Iran-Iraq War of 1980), Iran developed asymmetric warfare capabilities that utilized their strategic coastal location to counteract enemy forces. Iran's naval development has grown over the past few years in order to secure control of the Strait of Hormuz. The IRGC's naval arsenal includes submarines, mines, hundreds of small boats, and coastal cruise missiles capable of being deployed instantaneously from several naval bases. Independently from the IRGC, the Islamic Republic of Iran Navy also protects the Iranian coast. However, despite Iran's naval prowess, its land based combat forces lack the capacity to mobilize as proficiently as its navy. Please see Appendix A for a more detailed overview of Iran's military capabilities. These figures are best estimates provided by Department of Defense analysts and may not provide an accurate and complete account of Iran's military capabilities.

In recent years, Iran has invested more resources into its nuclear program, claiming that the future of the Iranian oil industry is in decline. Iran attributes the sanctions against it as the primary cause behind the decline in revenues from the oil trade they previously conducted with

---

[15] Salemi, Vahid. "Islamic Revolutionary Guards Corps (Quds Force)." New York Times on 3rd Oct. 2012. Retrieved September 12th, 2013. <http://topics.nytimes.com/top/reference/timestopics/organizations/i/islamic_revolutionary_guard_corps/index.html>

other international partners. As an alternative form of energy, Iran plans to use nuclear technology for electricity generation as well as for medical uses. Despite claims by the international community that Iran's nuclear development is to perpetrate aggression against its enemies, Iran contends that its nuclear program is peaceful, and has continued uranium enrichment despite continued sanctions. Much of the Iranian population believes it has a basic "right" to peaceful nuclear technology and that Western demands are both harsh and unfair[16]. Iran, however, has drastically enhanced its nuclear enrichment levels from 3-5% to 20%. This rapid rise has further sparked international concern, since Iran appears to be moving toward the high levels of uranium enrichment (over 90%) needed for nuclear weapons[17]. The Institute for Science and International Security believes that Iran's nuclear threat is more imminent, reporting that "Iran could produce enough weapons-grade uranium to make an atom bomb within two to four months and then would need an additional eight to ten months to build the device" i.e. Iran could build a nuclear weapon that would be significantly more destructive than the atom bomb used by the U.S. on Hiroshima and Nagasaki. To date, Iran could build up to 5 nuclear weapons given their supply of over 15,000 lbs. of low-enriched uranium[18]. A nuclear-armed Iran would be more assertive in its attempts to influence foreign and energy policies in the Persian Gulf, and Iran would provide greater support and potentially nuclear material for countries and movements that oppose Western interests. Additionally, Iran would likely threaten the United States with a nuclear attack and as they have stated in the past, attempt to destroy Israel.

---

16 Majd, Hooman: "The Ayatollah Begs to Differ: The Paradox of Modern Iran."
Page 119. Published by Doubleday NY in 2008.
17 Katzman, Kenneth: "Iran: U.S. Concerns and Policy Responses." Congressional Research Service on 5th September 2012. Page 28, Retrieved September 9th 2013.
<http://www.fas.org/sgp/crs/mideast/RL32048.pdf>
18 Katzman, Kenneth: "Iran: U.S. Concerns and Policy Responses." Congressional Research Service on 5th September 2012. Page 30, Retrieved September 9th 2013.
<http://www.fas.org/sgp/crs/mideast/RL32048.pdf>

Iran has repeatedly stated that its nuclear program is peaceful but thus far the country's belligerent actions have proven otherwise. As a result, many countries have placed sanctions on Iran, which have taken a toll on the country. Iran has offered to decrease its uranium enrichment levels in exchange for removal of certain sanctions, but Iran lacks credibility in following through with agreements given its history of neglecting recommendations made by the International Atomic Energy Agency (IAEA). Hence, no progress with respect to these negotiations has been made to this date. However, in light of recent possible action with regard to Syria and a change in leadership, Iran has indicated that it may be willing to negotiate with the United Nations with respect to its nuclear program. Recently, a landmark agreement with 51 signatories (and counting) was reached with respect to lifting certain sanctions on Iran in exchange for United Nations administered checks of Iran's nuclear facilities, however there remains significant skepticism to Iran's willingness to allow U.N. administered checks of its nuclear infrastructure.

United States sponsored Cyberwarfare against Iran

As discussed, the threat from Iran as a nuclear nation can hardly be overstated in light of their previous aggressions, provocative leadership, and sponsorship of terrorist groups intent on harming U.S. and Israeli interests in the Middle East. Apart from indirect, diplomatic conflict with Iran, the United States has implemented more direct measures against Iran through cyber-attacks. The Bush administration created the cyber-attack program "Olympic Games" to hinder Iran's nuclear development program out of fear that implementing sanctions would negatively harm the US and its allies' economy. Obama's administration accelerated the cyber-attacks and

"temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium"[19].

Despite the pressure that US cyber-attacks and sanctions have placed on Iran, the Iranian government has refused to yield its nuclear enrichment program, continuing to claim the program is peaceful; it also retaliated with a cyber-attack of its own. This cyber-attack breached Saudi Arabia's oil industry Aramco, as well as United States financial institutions, "erasing files on about 30,000 computers" of Aramco's systems and prohibiting some American bank customers from accessing their account[20]. Furthermore, on November 1, 2012, two Iranian Su-25 fighter jets fired at an unarmed American surveillance drone off the Persian Gulf[21]. Some political pundits consider this response a direct act of war. A nuclear-armed Iran could provide terrorist organizations such as Hezbollah with nuclear materials and could potentially use nuclear weapons to attack Israel and/or the United States. Thus, containment of Iran's developing nuclear abilities has been the focus of U.S. cyber weapons programs for the best part of the last decade. Next, we will discuss how Just War Theory is applicable to this scenario and why cyberwarfare conducted by the United States is just under the conditions of the Just War doctrine.

---

[19] Sanger, David E.: "Obama Order Sped Up Wave Of Cyberattacks Against Iran." The New York Times on 1st June 2012. Retrieved September 9th 2013. <http://www.nytimes.com/2012/06/01/world /middleeast/obama-ordered-wave-ofcyberattacks-against-iran.html?pagewanted=all>

[20] Shanker, Tom, and Sanger, David E.: "U.S. Suspects Iran Was Behind a Wave of Cyberattacks." New York Times on 13th October 2012. Retrieved September 10th 2013 <http://www.nytimes.com/2012/10/14/ world/middleeast/us- suspects-iranians were-behind-a-wave-of-cyberattacks.html?ref=stuxnet>

[21] Starr, Babara: "First on CNN: Iranian Jets Fire on U.S. Drone." CNN on 8th November 2012. Retrieved September 6th 2013. <http://security.blogs.cnn.com/2012/11/08/first-on-cnn-iranian-jets-fire-on-u-s-drone/?hpt=hp_t1>

Application of Just War Theory

There are some unique challenges to the application of Just War Theory in the case of United States sponsored cyberwarfare against Iran. These challenges rest primarily with the principle of *just cause* in jus ad bellum (justice of the war) and whether the United States had sufficient cause with respect to its cyber attacks on Iran's military and nuclear facilities. Like most wars in the modern political arena, there is a cluster of reasons, as opposed to a single root cause, behind a state's decision to engage in warfare. We know that in recent years, the looseness or plasticity of Just War Theory has allowed it to become more open-ended with regard to being permissive of war especially in cases where one reason alone does not satisfy the just cause principle.

Considering the U.S. cyber attacks against Iran, it would almost seem as if it is in violation of Just War Theory and that it would be fairly easy to argue that the United States had *no just cause* for its actions. Iran as a state is not engaged in any military conflict with the United States or its allies and has not attacked the United States in any way. Furthermore, Iran is not committing any heinous crimes against humanity or its own citizens. Indeed, many pacifists have deemed the American cyberweapons programs directed at such threats to be morally reprehensible and in violation of U.N. conventions on sovereign autonomy. However, such a simplistic rendering of the just cause principle ignores the fundamental logic upon which Just War Theory is built. One of the issues with the just cause principle is that its looseness can lead to unscrupulous states using a plethora of reasons to justify their aggressions. However, it is evident that the U.S. had a number of good (just) reasons to initiate the "Olympic Games", their cyberweapons program against Iran's military and nuclear facilities. First, Iran has been exceedingly belligerent in the world stage and is a known backer of numerous terrorist groups,

including the Hezbollah. Second, Iranian leadership has openly declared that Israel, a close ally of the United States, is to be "wiped off the map" – a clear threat to a large civilian population. Third, the incident involving two Iranian fighter jets shooting at a U.S. surveillance drone could be considered an act of war that would justify a proportional response. Last, development of nuclear weapons by Iran is a threat to the security of the U.S. considering the tenuous relationship between the two countries. These reasons combined, present an overriding reason with which the U.S. may pursue hostilities against Iran.

The question of *legitimate authority* does not arise in this case as it is well documented that the Olympic Games program was authorized initially by then President of the United States, George W. Bush and continued by his successor, President Barack Obama. We can only guess that retaliatory cyber attacks from Iran were directed by their Sovereign leader and if so, were justified in response. However, if the Iranian leader did not authorize the retaliatory cyber attacks, they would be deemed unjust under the Just War doctrine. However, the principle of legitimate authority is not very contentious in this case as we are principally focused on the actions by the United States. Scholars such as Randall Dipert have argued that the stealthy nature of cyber attacks makes the attribution of responsibility difficult and this is one of the failings of Just War Theory to address cyberwarfare. On the contrary, recent evidence has shown that cyberweapons are particularly sophisticated and are usually under the direct command of the upper echelons of government and their use is usually authorized directly by the head of state[22].

Other principles of jus ad bellum that we must consider include likelihood of success, proportionality, right intentions, and last resort. As discussed, efforts to negotiate with Iran, both in the past and present, have proved futile. Iran's enrichment of uranium to weapons-grade levels

[22] Libicki, Martin C.: "A matter of Degree: Who Can Authorize a Cyberattack?." Federation of American Scientists on January 9th 2013. Retrieved 28th November 2013. <http://www.rand.org/commentary/2013/01/09/FAS.html>

is in defiance of international law and it has refused to cooperate with the United Nations with regard to its violations despite several sanctions being placed upon it. It is evident that every step to avoid conflict was explored before the U.S. deployed its cyberweapons strategy. Not only is Iran famous for having used protracted negotiation as a delaying tactic in the past, but it also continued its uranium enrichment project while such negotiations were in progress – a clear indicator that it did not plan to enter into any agreement in good faith. Thus, the U.S. was justified in pursuing its aggressive cyberweapons program as a *last resort* to neutralize the threat of Iran's nuclear program.

With regard to the *proportionality* principle, it can be said that the cyber attacks on Iran were actually beneficial across the board – they reduced the threat of Iran's nuclear capabilities and did not have any known collateral effect on Iranian civilians (which is more than can be said of the economic sanctions placed upon the country). The proportionality principle in the case of jus ad bellum takes into account the cost and benefit of war. While it is typically difficult to estimate the cost of war due to the cost to human lives, it is far easier in this case as no human lives are being wagered. The most beneficial aspect of cyberweapons is that they usually take human lives out of the cost-benefit equation. As such, from a pure dollar cost perspective, using cyberweapons is far cheaper than using conventional forces (sending in troops, etc.) to minimize the efficiency of the Iran's program. Several documents leaked by Edward Snowden show that the U.S. mounted over 230 cyber attacks in 2011 as part of operation "GENIE" at a cost of $652 million: pennies on the dollar when compared to cost of military expeditions in the Iraq War[23].

[23] Gellman, Barton and Nakashima, Ellen: "U.S. Spy Agencies mounted 231 offensive cyber-operations in 2011, documents show." Washington Post on August 30th 2013 Retrieved on November 28th, 2013. < http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html>

Similar to proportionality, just war theorists also consider the *likelihood of success* before engaging in any form of conflict. The computer worm "Stuxnet" was used by U.S. and Israeli intelligence agencies to systematically target Iran's nuclear facilities with great success and there is significant evidence that suggests the U.S. was well aware of the probability of success when it launched the worm. While much of the information on the U.S. cyberweapons program is classified, a simple comparison of the size of the U.S. resources in the cyberspace to the information technology available to the Iranian government suggests that any such attempt would be met with success. Furthermore, the goals of the program were remarkably low in expectation – U.S. intelligence was directed to slow down Iranian efforts to enrich uranium and they were given a broad timeframe within which such a program needed to achieve success. Thus, any standard regarding the likelihood of success would have been met in this situation and need not be discussed further.

Last, we arrive at the question of whether the U.S. had the right intentions behind deploying the Olympic Games program against Iran. While motive behind aggression has been a contentious issue with Just War Theory in past wars, it is evident that the U.S. did not conduct cyber attacks on Iran for any purpose other than to reduce the threat of its illegal nuclear program to its citizens and allies. The Stuxnet worm was not built to steal confidential information and had no purpose other than to destabilize or destroy Iranian nuclear enrichment infrastructure. The U.S. has not conducted any operations that were intended to infringe upon Iranian sovereignty by either land or sea. With no territorial ambitions and the safety of its allies in the crosshairs, the U.S. appears to have had the right intentions with respect to its cyber aggressions against Iran.

From the information presented above, we would hope most would agree that the U.S. satisfied the principles of jus ad bellum. However, we must also consider the principles of jus in

bello (justice in the war), especially the principle of discrimination. The principle of discrimination has been used by the Geneva Convention to adjudicate cases of atrocity committed by armies against civilians. In the situation presented, it would be easy to suggest that since the U.S. targeting Iranian military infrastructure with its worm, it satisfies the tenants of the principle of discrimination. However, it is known that Stuxnet and another virus known as "Flame" eventually spread outside the core Iranian government network, affecting personal computers and causing damage to civilian property. The virus didn't stop there: it went on to affect the cloud infrastructure of Russian civilian nuclear power plants, causing widespread damage and potential environment harm from a core meltdown[24]. While U.S. intentions were never to cause any harm to civilian infrastructure (especially not in another country), the uncontrolled nature of cyberweapons has been an issue of concern expressed by those who believe the U.S. should not engage in cyberwarfare. There are several arguments to be made, both from proponents and detractors of the U.S. cyberweapons policy, but is clear that in this situation the U.S. failed to isolate its virus to military targets and violated the principle of discrimination.

The case study of U.S. cyberwarfare against Iran is interesting as it could be said that the cyber attacks were a *preventive* measure. As we know, preventive attacks are not allowed under the Just War doctrine; *preemptive* measures are allowed however. This is because technological advances such as the development of cyberweapons are relatively new and Just War theory was not written at a time when such weapons were even considered. Just war theorists have previously defined a preventive attack to be one "designed to stop an expected enemy attack in

[24] 21st Century Wire: "More Stuxnet: US–Israeli Computer Virus Infected Russian Civilian Nuclear Power Plants." 21stCenturyWire.com on November 13th 2013. Retrieved November 21st, 2013. <http://21stcenturywire.com/ 2013/11/13/more-stuxnet-us-israeli-made-virus-infected-russian-civilian-nuclear-power-plants/>

the distant future" where not much is defined in the way of what timeframe would allow for a preemptive strike[25]. However, a preemptive strike may be defined as an attack that counters "preparations such as fueling airplanes, loading them with munitions and moving major ground forces armed and ready for attack towards the border are being made" and if concern of a future attack is augmented by intelligence efforts[26]. In our case, the U.S. has ample evidence from both intelligence assets in the region and from the outspoken statements by Iran's leadership that Israel is the focus of Iranian aggression. What is not clear is the timeframe of such aggression, particularly in consideration of Iran's nuclear program. I would argue that the U.S.–Israeli program to destabilize Iranian nuclear infrastructure is preemptive when one considers how easily nuclear fission can be deployed and the speed of ballistic systems available to Iran. Furthermore, the impact of such an attack would be far more devastating that anything previously encountered, except for the attacks on Hiroshima and Nagasaki, and the U.S. must take measures to protect its allies from such devastation. The provocative statements made by the Iranian leadership clearly demonstrate urgency for aggression, which indicates that any attempt to delay or destroy Iran's nuclear capabilities must be preemptive in nature. Thus, taking into account the various tenets under the Just War Theory, the U.S. was justified in launching a cyber attack on Iran but guilty with regard to the civilian damage its program was responsible for.

[25] Fotion, Nicholas: "War & Ethics: A New Just War Theory." Page 13. Continuum International Publishing 2007.
[26] Fotion, Nicholas: "War & Ethics: A New Just War Theory." Page 13. Continuum International Publishing 2007.

CASE STUDY: SYRIA

There has been significant debate regarding the Syrian Civil War and whether the United States should get involved as it did in Libya and in other war-torn regions around the globe. Considering the question from an ethical theory perspective, and more precisely, from the viewpoint of a just war theorist, one would say that the United States has no good (just) cause to get involved. This is because Just War Theory does not provide a basis for any state to be involved in conflict on grounds of idealism, religion, etc. and does not consider any such reason to provide "just cause" for aggression. Thus, on the surface, one would say that the United States should not get involved in the conflict. However, by any moral standard, the atrocities being committed by Assad loyalists against the civilian population cannot be dismissed. This brings us to the tenet of Just War Theory that allows for a country to intervene in the affairs of another on humanitarian grounds. As it is with other cases discussed in this paper, it is important to furnish the reader with some information before we delve into the applicability of Just War Theory to the situation described in this case:

a. Background of the relations between the United States and Syria in order to demonstrate that there is no historical reason/bias due to which the U.S. may choose to intervene in Syria as opposed to the humanitarian cause.
b. An assessment of Syrian military capability in order to demonstrate that Syria possessed the capability to use chemical weapons against its citizens and the current regime has the capability to defend itself against foreign military action due to support from allies such as Russia. This will be especially relevant in the discussion of the proportionality principle and likelihood of success of U.S. cyberwarfare programs in comparison to any conventional military operations.

c. A brief summary of the Syrian Civil War – this allows us to contextualize the need for U.S. intervention and demonstrate why there is a just cause for such intervention.

Relations between Syria and the United States

As with many states in the region, Syria–United States relations have been marked with controversy since the U.S. recognized Syria as an independent country in 1946 and established a consulate in Damascus. In the years that followed, the U.S. tried to influence the Syrian government to be more representative through a 'Political Action Team' after which the U.S. tried to overthrow the government[27]. Such actions, augmented by the failed Central Intelligence Agency ("CIA") 1957 coup to replace then Syrian President Adib Shishakli, are considered to be major factors in the contentious relationship between the two countries today. After the failed 1957 coup d'état, Syria and the U.S. recalled their respective Ambassadors. The Six-Day War or the Israeli-Arab War as it is known in the region further strained relations between the U.S. and Syria. It was only after the Syrian-Israeli disengagement agreement in 1974 that then U.S. President Richard Nixon visited Syria on an official trip and Syria and the U.S. re-constituted formal relations.

While Syria has cooperated with the U.S. in the 'War on Terror', its opposition to the war in Iraq led to deterioration in relations in the recent past. Furthermore, Syria has becomes a target of international criticism due to its apparent sponsorship of international terrorist groups such as the Hamas, Palestinian Islamic Jihad, Hezbollah, etc. and the poor human rights record associated with its secular dictatorship government[28]. The U.S. has also condemned Syria for allegedly providing SCUD missiles to Hezbollah forces in Lebanon and encouraging terrorist

[27] Curtis, Adam: "The Baby and the Baath Water." BBC on June 16th 2011. Retrieved on November 13th 2013. < http://www.bbc.co.uk/blogs/adamcurtis/posts/the_baby_and_the_baath_water>

[28] United States Department of States, Office of the Coordinator for Counterterrorism: "Country Reports on Terrorism 2009." Page 195. Retrieved on November 13th 2013. <http://www.state.gov/documents/organization/141114.pdf>

operations there[29]. Due to its presence on the list of state sponsors of terrorism, Syria has been the subject of several economic sanctions by the U.S. further adding to the acrimonious relationship between the two states. Also, Syria is widely believed to have provided safe haven to terrorist groups fleeing from U.S. operations across Iraq and allowed free movement of supporting terrorist groups across their borders into Iraq.

In light of the events surrounding the ongoing Syrian Civil War, there has been a marked escalation in tensions between the U.S. and the current Syrian regime. Initially the U.S. believed the Syrian response to the protests was peaceful and believed the Syrian government would heed the requests of its people[30]. Such hopes were short-lived as Basher-Al-Assad's regime began a harsh crackdown on the protesters, which soon escalated into the ongoing civil war that has engulfed the country. During this time, President Barack Obama has called for Assad to step down from the position of President while the U.S. has pushed the United Nations to adopt stringent measures against Syria in light of the crackdown. Russia and China, allies of Syria, have opposed such measures with their veto powers[31]. This is considered to be in reaction to increasing American influence in the region particularly through Saudi Arabia – a supporter of the opposition to Assad's government in the Syrian Civil War. It also suggests that Russia and China may become active supporters of Assad in a situation reminiscent of the Cold War where the Western states were pitted against the Eastern Bloc in similar situations across the Middle East. One of the concerns voiced by Russia was that the resolution proposed by the United States

---

[29] Fletcher, Holly: "State Sponsor: Syria." Council on Foreign Relations in February 2008. Retrieved on November 13th 2013. < http://www.cfr.org/syria/state-sponsor-syria/p9368>

[30] Goodenough, Patrick: "Syrian President Assad Regarded As a 'Reformer', Clinton Says." CNS News on March 28th 2011. Retrieved on November 13th 2013. < http://cnsnews.com/news/article/syrian-president-assad-regarded-reformer-clinton-says>

[31] Horn, Jordan: "US 'outraged' after Russia, China veto Syria UN resolution." The Jerusalem Post on October 5th 2011. Retrieved on November 17th 2013. < http://www.jpost.com/Diplomacy-and-Politics/US-outraged-after-Russia-China-veto-Syria-UN-resolution>

could provide precedent for Western states to stage a military intervention in Syria, similar to France's role in the Libyan conflict[32]. This is important as it indicates that Russia may be willing to side with the current Syrian regime if the situation escalates even further into a military conflict encompassing several world nations. Finally, in October 2011, the U.S. recalled Robert S. Ford, its Ambassador to Syria, due to concerns surrounding his personal safety and forced Syrian officials in Washington to leave the country following the Houla massacre, a gross violation of human rights by that is discussed in greater detail later in this chapter[33].

Syria's military capability and ties to Russia, Iran & Other Paramilitary Groups

Syria's military strength is an important measure that can be used to determine the opposition the U.S. or any Western state will face if it chooses to intervene in the Syrian Civil War by conducting conventional military operations. The Syrian Armed forces consist of the Syrian Arab Army, Syrian Arab Navy, Syrian Arab Air Force, Syrian Arab Defense Force, and several other paramilitary forces. The Syrian Constitution dictates that the President of Syria serves the Commander-in-Chief of the armed forces. Recruitment to the military is in the form of conscription where all males serve in the military after attaining the age of 18 years[34]. The mandated service for conscripted soldiers is currently 18 months, although it has previously been as high as 30 months.

The Syrian Armed Forces have undergone significant turmoil since the onset of the civil war in the country. Theoretically the Syrian army was known to consist of 178,000 troops,

---

[32] Horn, Jordan: "US 'outraged' after Russia, China veto Syria UN resolution." The Jerusalem Post on October 5th 2011. Retrieved on November 17th 2013. < http://www.jpost.com/Diplomacy-and-Politics/US-outraged-after-Russia-China-veto-Syria-UN-resolution>

[33] BBC News: "Houla deaths: Western states to expel Syrian diplomats." BBC News Middle East on May 29th 2012. Retrieved on November 13th 2013. < http://www.bbc.co.uk/news/world-middle-east-18252818>

[34] GlobalSecurity.org: Syria–Overview. <http://www.globalsecurity.org/military/world/syria/overview.htm>

including 110,000 in ground troops, 5,000 in the Navy, 27,000 in the Air Force, and 36,000 in Air Defenses before several units deserted the Assad regime and joined the 'Free Syrian Army', the banner under which the opposition forces are organized. Additionally, the Army had 314,000 personnel in reserve and could swell the ranks of the Navy by 4,000 men, the Air Force by 10,000 men, and the Air Defenses by 20,000 men[35]. However, current estimates of the forces loyal to the Assad regime suggest that approximately half of the Syrian Armed Forces have deserted and either joined the opposition or abandoned the government. Despite such departures, the Syrian Armed Forces still remain a formidable force, especially with Russia as an ally.

Syria's military is mainly equipped with Soviet-era weapons provided by Russia. The Syrian army has approximately 4,950 tanks and the Air Force maintains a fleet of about 555 Soviet fighter planes in varying degrees of operational readiness. The Syrian chemical arsenal is known to be one of the largest in the Middle East, if not the world, and has never been the subject of international inspection. This is because Syria is not a signatory to Chemical Weapons Convention and is not a member of the Organization for the Prohibition of Chemical Weapons (OPCW)[36]. Syria's chemical program was developed primarily as a response to Israel's nuclear program and was supported significantly by Russia in the 1990s and Iran in the mid-2000s. The arsenal is believed to contain large quantities of older chemical agents such as mustard gas along with newer nerve agents such as Sarin gas and VX.

Finally, we must consider the alliances between Syria and states such as Russia, Iran, and China as well as paramilitary groups such as the Hezbollah. It is clear from the U.N. veto that both Russia and China intend to support Syria diplomatically, if not in combat. Russia can be

---

[35] Oster, Adrien: 'Syria's Army: What The West Will Face In Case of Intervention." HuffPost France on August 29th 2013. Retrieved on November 17th 2013. < http://www.huffingtonpost.com/2013/08/29/syria-army_n_3837031.html>

[36] Organisation for the Prohibition of Chemical Weapons: "Non–Member States." Retrieved November 17th 2013. < http://www.opcw.org/about-opcw/non-member-states/>

considered a military ally as it has been a big provider of weapons to Syria in the past and continues to support the regime during the Civil War. Iran is also supportive of the current Iranian government while the Hezbollah has actually fought against the opposition alongside troops loyal to Assad. In a show of force, Syrian Foreign Minister Walid Moualem suggested that Syrian military capabilities would "surprise" the world and was confident that Russia had not abandoned Syria due to the continued relations between the two countries[37].

The Syrian Civil War

As one may be aware, the Syrian Civil War began as an uprising seeking to oust the Ba'ath government from power. While exact dates remain are unclear, the conflict began in March 2011 and is ongoing to the present day. Initially the protests against the Syrian regime under Bashar-al-Assad were part of the larger 'Arab Spring' movement in the Middle East and revolved around issues of corruption and human rights. The Syrian military soon cracked down on protesters but this escalated the situation as many protesters took up arms against the military. Soon, troops from the military began to defect to join the protesters and by July of 2011, the protests had grown into an armed insurgency by the protesters.

The Free Syrian Army ("FSA"), a group that represented the primary opposition army, was formed also formed at this time[38]. Following the formal recognition of this group by some Western states, the conflict between Assad-loyalists and the FSA intensified. The opposition forces received support from Turkey and the FSA and Syrian Army engaged in the first of many skirmishes in towns and cities near the Turkish border. The Syrian Army began the use of heavy

---

[37] France24: "Syria warns of 'surprise' military capabilities." France24 International News on August 28th 2013. Retrieved November 17th 2013. < http://www.france24.com/en/20130828-syria-surprise-military-capabilities-russia-iran-usa>

[38] Boxx, Lt. Colonel Edward S., USAF: "Observations on the Air War in Syria." Page 152. Washington Institute, March–April 2013. Retrieved on November 19th 2013. <http://www.washingtoninstitute.org/uploads/Documents/ opeds/Boxx20130301-AirSpace.pdf>

artillery in many of the encounters and the resulting collateral killings of civilians induced sympathy for the rebel cause. January 2012 saw the FSA and rebels engage the Syrian Army in the neighborhoods of Damascus, validating their growing ranks by taking the conflict to the nation's capital. A negotiated ceasefire during the months of April–May 2012 did not last due to the Houla massacre where it is believed that pro-government militia executed hundreds of civilians. The massacre had been preceded by the Syrian Army's use of heavy armament fire against rebel-held towns without any care for the collateral damage to the civilian population in these towns.

The United National Human Rights Council voted by a 41–6 majority to condemn Syria for the Houla massacre and the U.S. advocated for stringent measures against Assad's regime in the Security Council. While Syria has maintained that rebel militia or the Al-Qaeda in the region caused the Houla massacres, witness accounts suggest otherwise. Furthermore, the Syrian government's position became weaker following reports by the opposition that the regime had used chemical weapons against the opposition forces. Reports by U.S. intelligence analysts put the death toll of the attack at over 1,400 people and suggested that the "use of chemicals in recent months had become part of the normal military strategy whenever government forces were unable to push back rebel offensives or break defensive fortifications."[39]

Application of Just War Theory

At the very outset, it is evident that the case of Syria is significantly different from the cases concerning Iran and North Korea discussed in this paper. Here, we are using Just War Theory to show how the use of cyberweapons may present a more ethical way for the United States to intervene into the situation in Syria. This is a two-fold task, as we will demonstrate that:

[39] Warrick, Joby: "More than 1,400 killed in Syrian chemical weapons attack, U.S. says." Washington Post on August 30th 2013. Retrieved on November 19th 2013. <http://articles.washingtonpost.com/2013-08-30/world/41606663_1_obama-administration-u-s-intelligence-analysts-syrian-government>

a. The use of cyberweapons is justified under Just War Theory and satisfies the principles of jus ad bellum and jus in bello.
b. The use of conventional military to intervene in the situation would not be justified under the Just War doctrine and therefore, the use of cyberweapons is the more ethical and effective solution.

Let us consider the just cause principle of jus ad bellum. As we know there are several reasons that may be used to satisfy just cause. In the case of Syria, the United States is justified in staging an intervention on humanitarian grounds, as it is clear that the current Syrian regime is conducting "genocide-like activity" against a large group of its own citizens[40]. The mass massacre of civilians through the shelling of rebel-held towns and use of chemical nerve agents serves as evidence of such activity. As Just War theorists would argue, humanitarian intervention can be difficult to justify as the intervention often looks like aggression. This is because the neither the intervening nation nor its allies are under attack and there is no threat of being attacked in the near future. However, such action is usually justified by the notion that the costs of not intervening (human lives, etc.) would be far greater than the cost of a conflict where the end goal is to end the suffering of innocent civilians.

Just War Theory mandates that any aggression must be a last resort in order to be justified. Considering the worsening situation in Syria, it could be said the situation could not be more dire for the civilians embroiled in the conflict in the country. A failed ceasefire and escalating conflict with several nations in the region getting involved shows that there is no time for the U.S. to orchestrate any agreement between the FSA and Assad regime. Taking the situation into account it would seem that the last resort principle is satisfied in this case.

[40] Fotion, Nicholas: "War & Ethics: A New Just War Theory." Page 13. Continuum International Publishing 2007.

The application of the principles of proportionality and likelihood of success are particularly interesting in the case of Syria as opposed to Iran or North Korea. This is because both principles when applied to the circumstances surrounding Syria will demonstrate that the use of cyberweapons by the U.S. against Syrian military infrastructure would be justified whereas conventional military operations by the U.S. against the Syrian regime may not be justified under Just War Theory.

First, let us take the principle of proportionality. Under jus ad bellum, the benefits of the war must exceed the cost of war. While it has already been established that in the case of humanitarian intervention, the benefits almost always considered to outweigh the costs, the alliance between Syria and Russia complicates this situation. One of the reasons the U.S. and other Western powers have not staged any sort of military intervention in Syria is because of the friendly relations between Syria and Russia. On a diplomatic level, the U.N. Security Council cannot act against Syria because Russia and China have vetoed any such measure. If the U.S. were to engaged in conventional warfare against Syria, it could have the makings of a third world war with the U.S. and its allies pitted against Russia and its allies defending the Syrian regime. The costs of such a war, while unlikely to take place, would be far greater than can be estimated. Considering both the U.S. and Russia have advanced nuclear capabilities, the costs could well exceed the benefits of any intervention that triggers a conflict between these two world powers. However, engaging in cyberwarfare, which is stealthy in nature, offers the U.S. a way to intervene in the war without endangering any American or civilian lives, while also not confronting Russia in a manner that involves the two countries in a direct military conflict. The low cost of implementing cyberweapons against targets has been well documented and such an

attack could hamper the Syrian Army's communications and infrastructure and provide the opposition with the opportunity to improve their position in the conflict.

Second, let us consider the likelihood of success of an American intervention into the conflict. As many observers have noted, the Syrian Army would be no match for the U.S. military on its own. However, with Russian support, the likelihood of success of a U.S. military operation is significantly lower. A case could be made that intervention by both the U.S. and Russia could lead to a stalemate in the region, which would exacerbate the crisis. A cyber attack by the U.S. would have a much greater chance of success than any conventional military operation. It is widely believed that the U.S. has one of the most formidable arsenals of cyberweapons in the world and such an attack would not be easily traced back to the U.S. conclusively. A cyber attack would also be more tenable to the U.S. public whose opinion, as polls show, is strongly against the U.S. getting involved in another conflict in the Middle East. Recovering from a financial crisis and relations with allies at a low due to illicit surveillance by the National Security Agency ("NSA"), the U.S. is in no position to wage a conventional war against an armed Syria backed by Russia and its allies. Therefore, the only justifiable way for the U.S. to intervene in the Syrian Civil War when considering the likelihood of success principle is to use a cyberweapon and cripple Syrian military infrastructure.

Finally, the last two principles of jus ad bellum we must consider are those of right intentions and legitimate authority. Similar to the case involving Iran, the question of legitimate authority does not arise in this case as any act of cyberwarfare by the United States would have to be authorized by the President. As was the case with the infamous 'Olympic Games' cyberweapons program the U.S. unleashed against Iran, President Obama would be responsible for initiating a cyber attack against Syria and his order would be executed U.S. intelligence

agencies such as the Central Intelligence Agency ("CIA"). Since the U.S. would intervening in Syria on humanitarian grounds the principle of right intentions would also be satisfied. It could be argued given the history of Syrian–U.S. relations that this maybe a case of the U.S. siding with the opposition forces in order to influence Syria to form a more representative government. However, such an argument would be rendered invalid considering President Obama's own stance that the U.S. would only get involved if it could be proved the Syrian regime had used chemical weapons against its citizens i.e. committed a crime against humanity[41]. Thus, by eliminating the possibility of intervention unless it could be proven that Syria was committing genocide against its people, President Obama effectively proved that any intervention from the U.S. would be for the right reasons.

In this discussion of the Syrian Civil War, we have used the principles of jus ad bellum to demonstrate that the use of cyberweapons by the U.S. to intervene in the civil war would be justified. While it is impossible to predict for certain if the U.S. will be able to satisfy the principle of jus in bello if it decides to intervene in Syria, we can make an assumption that using controlled cyberweapons, the U.S. should not have any difficulty satisfying the principle of discrimination. Since any intervention would on humanitarian grounds, it would be particularly abject if the U.S. itself was guilty of harming the civilians it chose to intervene on behalf of. One could say that intervention using controlled cyberweapons (unlike the Stuxnet virus that went rogue in Iran) could better satisfy the principle of discrimination as it could be made to only affect military systems as opposed to civilian infrastructure. Furthermore, in the case of conventional weapons, there is always the possibility of collateral damage to civilians, which is a risk that could be avoided by the use of cyberweapons.

---

[41] Pleitgen, Frederik and Cohen, Tom: " 'War-weary' Obama says Syria chemical attack requires response." CNN on August 30th 2013. Retrieved on November 18th 2013. <http://www.cnn.com/2013/08/30/world/europe/syria-civil-war/>

Thus, this case study is different from most that use Just War Theory to assess the just nature of wars as it employs the Just War doctrine to make a case for aggression using cyberweapons by a state. While most of Just War Theory is retroactively applied, our analysis uses the principles of jus ad bellum and jus in bello to make the argument that the United States should intervene in Syria on humanitarian grounds using a cyberweapons strategy. We are also able to determine that the use of cyberweapons would be better from an ethical perspective under the Just War doctrine than the use of conventional military tactics. Our discussion also servers to counter some of the claims made by critics that Just War Theory is too outdated to be applicable today by demonstrating that the Just War doctrine could be used to make a case for the use of newer technologies such as cyberweapons in modern-day conflict situations.

CASE STUDY: NORTH KOREA

North Korea or the Democratic People's Republic of Korea ("DPRK") has been central to the discussion surrounding the foreign policy of the United States in South-East Asia for the better part of the last decade. The aggressive rhetoric coming out of Pyongyang, the nation's capital, in recent months has sparked fears of a conflict on the Korean peninsula. This situation has been escalated by North Korean cyber attacks against South Korea and U.S. military infrastructure. In this chapter, Just War Theory is applied to determine if the United States and South Korea are justified in responding to cyber attacks by North Korea and whether cyber attacks provide just cause for retaliation.

Relations between North Korea and the United States

North Korea has been an interesting case in the global political theatre following its founding in 1945. Created after Japanese rule ended on the Korean peninsula following World War II, North Korea is a totalitarian dictatorship ruled by Kim Jong-un, the son of the deceased Kim Jong-il. International relations between the current North Korean regime and most Western powers are a result of Cold War era politics following the Korean War. However, in recent years, relations between North Korea and the West have been dominated by North Korea's increasingly belligerent nuclear policy under which it has conducted three tests of nuclear weapons and developed long-range ballistic missiles to serve as delivery vessels for atomic weapons.

The United States does not officially have any formal relations with North Korea. Instead, it relies on Sweden, which maintains an embassy in Pyongyang to represent its diplomatic interests in North Korea. Relations between the two countries have been particularly contentious in the recent past, as North Korea has threatened to annihilate South Korea and strike

at the U.S. with long-range nuclear weaponry[42]. In what could almost be considered a declaration of war, North Korea made it clear that it could attack South Korea without warning and was withdrawing from the armistice that ended the Korean War in 1953. This has been in response to the U.S. leading a successful charge at the United Nations to sanction North Korea for its third nuclear test, which went against U.N. regulations[43]. It has been suggested that most of Pyongyang's threats may be similar to a strategy from its past when North Korea was able to secure concessions and aid from the U.S. in return for ending its nuclear weapons programs. Other experts believe North Korea simply wants to be recognized as a nuclear state and is using nuclear threats as a deterrent in case of military action by the U.S. or South Korea.

The history of U.S. relations with North Korea presents a pattern of mistrust on both sides. In the past, the U.S. has maintained a nuclear arsenal of over 900 nuclear warheads in South Korea for possible use against North Korea. The introduction of such atomic weapons into the Korean peninsula was a direct violation of the Korean Armistice Agreement. This prompted Pyongyang to prepare extensive underground fortifications and to move its conventional forces to the border for potential hostilities against the U.S. forces stationed in South Korea[44]. Furthermore, North Korea requested that the Soviet Union and China, its allies at the time, help it develop nuclear capabilities. This led to Russia helping Pyongyang develop a peaceful nuclear energy program. The tensions that surround nuclear proliferation in the Korean peninsula would not be revisited until the early 1990s when North Korea blatantly unloaded core nuclear material

---

[42] CNN Staff: "North Korea threatens to strike without warning." CNN on April 15th 2013. Retrieved on November 23rd 2013. < http://www.cnn.com/2013/04/15/world/asia/north-korea-ultimatum/index.html>
[43] The New York Times: "In Focus: North Korea's Nuclear Threats." The New York Times on April 16th 2013. Retrieved November 23rd 2013. <http://www.nytimes.com/interactive/2013/04/12/world/asia/north-korea-questions.html?_r=0>
[44] Selden, Mark and So, Alvin: "War and State Terrorism: The United States, Japan, and the Asia-Pacific in the long Twentieth Century." Pages 77-79. Published by Rowman & Littlefield in 2003.

from one its reactors, providing it with enough nuclear fissile material for several nuclear payloads.

North Korea initially became a signatory to the Nuclear Non-Proliferation Treaty ("NPT") as a non-nuclear weapons state. However, U.S. intelligence reports prompted the International Atomic Agency ("IAEA") to request an inspection of North Korean nuclear facilities; a request that was refused by Kim II Sung and led to North Korea's withdrawal from the NPT. Since then talks between the U.S. and North Korea have largely fallen through although the situation on the peninsula was considered stable. Unfortunately, this uneasy peace was short-lived as North Korea resumed nuclear activities in its Yongbyon facility arguing that the U.S. had not satisfied the conditions of previous agreements that involved sending aid to the country. Following Kim Jong-il's death in 2012, North Korea conducted a missile test, widely believed to have the range to reach the western seaboard of the United States. Indeed, Kim Jong-un has stated that American bases in the Pacific are the potential targets of a missile attack[45]. Furthermore, Pyongyang has declared that any discussions surrounding its nuclear weapons program would only be conducted after U.N. sanctions on the country are lifted and the U.S. removes its forces from South Korea[46].

North Korea's military and nuclear capability

It is widely known that North Korea has one of the largest standing armies in the world. The Korean People's Army ("KPA") consists of the Ground Force, the Air Force, the Strategic Rocket Forces, the Special Operation Force, and the Worker Peasant Red Guards. It has over 9

[45] MacAskill, Ewen: "US warns North Korea of increased isolation if threats escalate further". The Guardian on March 29th 2013. Retrieved November 12th 2013.
<http://www.theguardian.com/world/2013/mar/29/us-condemns-north-korea-threats>
[46] Sang-Hun, Choe: "North Korea Sets Conditions for Return to Talks". The New York Times on April 18th 2013. Retrieved November 17th 2013.
<http://en.wikipedia.org/wiki/North_Korea_US_relations#cite_note-63>

million personnel across these five divisions as well paramilitary groups under the Pyongyang regime's control. North Korea recruits through mandatory conscription for males and partial conscription for females, with the average service requirement being between 3 – 5 years. It has been estimated that approximately 40% of the entire population of the DPRK are part of one of one of the branches of the military. The budget of the KPA has been estimated to be around six billion U.S. dollars.[47] Some commentators suggest that this sum may represent up to 30% of the DPRK state budget. A recent report submitted by the Department of Defense asserts that "North Korea's large, forward positioned military can initiate an attack against the Republic of Korea with little or no warning, even though it suffers from resource shortages and aging equipment."[48] According to the report, the DPRK is making significant efforts to upgrade its conventional weapons and has "reinforced long-range artillery forces near the de-militarized zone" that have the capability of striking at targets in South Korea and Japan. Assessments of the DPRK's military strength from recent military parades show that North Korea has procured new infantry and group weaponry. North Korea's Air Force operates over 1200 active aircraft, mostly comprised of Soviet MiG–29s and Kazakh MiG–21s. It's aging ground and air forces have led the DPRK to focus on improving its surface-to-air missile capabilities and concentrate a greater portion of its resources to its ballistic missile development program.

North Korea's ambitious objectives with regard to its ballistic missile program and development of the TD-2 rocket have increased fears of the DPRK's ability to strike at targets as far as the United States with nuclear warheads. The DPRK is estimated have a little under 200 ballistic missile launchers with a maximum range of over 2,000 miles. However, concerns

[47] Institute for Science and International Security: 'Fast Facts about North Korea". Retrieved November 6th 2013. < http://isis-online.org/mapproject/country_pages/northkorea.html>

[48] Department of Defense: "Military and Security Developments involving The Democratic People's Republic of Korea". Page 7. Annual Report to Congress 2013. <http://www.defense.gov/pubs/report_ to_congress _on_military_and_security_developments_involving_the_dprk.pdf>

surrounding North Korea's capabilities are mainly focused on its "Weapons of Mass Destruction" ("WMD") programs. North Korea has conducted nuclear tests in 2006, 2009, and in early 2013 and continues to invest in nuclear enrichment infrastructure. The DPRK is also believed to have invested extensively in chemical and biological weapons programs, having acquired the ability to produce mustard gas in the mid-1900s. Consensus estimates suggest that the DPRK's stockpile of biochemical weaponry ranges between a minimum of hundreds of tons to a maximum of a few thousand tons. It also has eight biochemical production facilities that can be used to create varieties of nerve agents.

In recent years, North Korea has been one of the few countries (including the United States), to invest heavily in unconventional military infrastructure such as cyber weapons and other advanced technologies such as an electromagnetic pulse ("EMP") arsenal. According to South Korean intelligence, the DPRK has purchased EMP weapons from Russia and could, at minimum, damage electronic equipment and military infrastructure south of the demilitarized zone on the Korean peninsula[49]. Such developments suggest increased emphasis on destabilizing electronic infrastructure as a military priority. The DPRK controlled Korean Central News Agency has suggested that the development of cyber weapons in North Korea is in direct response to the U.S. cyber weapons program[50]. It is believed such weapons could be used to blackout U.S. and South Korean communications and throw the joint armed forces into disarray, providing North Korea's massive ground force with an opportunity to seize control of the South. Lastly, The National Intelligence Service, South Korea's version of the CIA, stated that North

[49] Anthony, Sebastian: "North Korea obtains EMP weapons from Russia, could now melt most of the electronics in Asia". ExtremeTech on November 7th 2013. Retrieved November 19th 2013. <http://www.extremetech.com/extreme/170563-north-korea-emp>

[50] North Korea Tech: "North Korean newspaper hits out at U.S. cyberwarfare policy". Retrieved November 28th 2013. <http://www.northkoreatech.org/2013/08/12/north-korean-newspaper-hits-out-at-u-s-cyber-warfare-policy/>

Korea has manned "cyber strike organizations" that it can mobilize in a war, fueling speculation that such cyber strike teams could disrupt aircraft GPS systems and use Trojan viruses to disrupt power networks and supply systems[51].

North Korea (DPRK) sponsored cyberwarfare against South Korea

Since taking power, Kim-Jung-un has been unexpectedly aggressive in his approach to ruling North Korea in comparison to his father, Kim-Jung-il. In the last two years, North Korea has undertaken long-range missile and underground nuclear tests while consistently threatening the U.S. and South Korea with destruction. While such rhetoric was initially dismissed as propaganda, recent cyberattacks against South Korea have forced intelligence experts to reconsider their initial positions. The attacks that began as simple Denial-of-Service (DoS) hacks have become increasingly sophisticated and estimates suggest that they have cost South Korea more than 800 million U.S. dollars already[52]. Increased tensions between the two countries due to such attacks have escalated the threat of war on the Korean peninsula. According to Jarno Limnéll, Director of cyber-security for Finland-based Stonesoft, "Actions in the cyber world easily escalate to warfare of threats of was, as the situation on the Korean peninsula demonstrates."[53] Concerns surrounding the DPRK's cyberweapons programs are mainly focused on the capability of North Korea's hackers to deploy cyberweapons with sophistication akin to Stuxnet, the virus used by the U.S. against Iran's nuclear facilities. Such weapons would give North Korea the ability to target U.S. and South Korean communications by damaging military

---

[51] ChosunMedia: "N. Korea Boosting Cyber Warfare Capabilities". The Chosun Libo on November 5th 2013. Retrieved November 18th 2013.
<http://english.chosun.com/site/data/html_dir/2013/11/05/2013110501790.html>

[52] Hern, Alex: "North Korean 'cyberwarfare' said to have cost South Korea £500m". The Guardian on October 16th 2013. Retrieved November 11th 2013.
<http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea>

[53] Rundle, Michael: "Cyber War Threatens Real-World Conflict in Korean Peninsula – And The North Might Be Winning". The Huffington Post on October 4th 2013. Retrieved November 11th 2013.
<http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea>

infrastructure used to control satellites, provide navigational and logistics support to forward divisions of the army, and aid many other components of the defensive fortifications of South Korea. The increasing ambition and scale of North Korea's hackers was revealed when South Korea's defense ministry released information that 30,000 computers in the country were hit by an attack in March 2013 – bringing down the operations of six banks and disrupting financial services across the nation[54]. The possibility that such cyberattacks could be used to pave the way for a North Korean invasion of South Korea – a stated goal of the Pyongyang regime, is driving the U.S. and South Korea to build up their cyber defenses. South Korean media is reporting that the country will be increasing the number of cyberwarfare experts in its "Cyber Command", a special unit of the military that was launched in 2010[55]. While the media have dubbed the preparations as a prelude to war, it is important to note that South Korea and North Korea are still technically at war, as the 1953 Armistice agreement was not a peace treaty between the two.

Application of Just War Theory

In this case, Just War Theory is not being applied to determine if the cyberattacks by the United States against a state are justified or whether the use of cyberweapons by the U.S. to intervene in a humanitarian crisis is better alternative to a conventional military response. Indeed, this case affords an opportunity to apply Just War Theory to a situation where two sides armed with nuclear weapons could go to war: a mutually assured destruction ("MAD") scenario. This situation has grave implications for any action by either side that could lead to the use of nuclear weapons and Just War Theory would not find any MAD scenario to be just under either

---

[54] Hern, Alex: "North Korean 'cyberwarfare' said to have cost South Korea £500m". The Guardian on October 16th 2013. Retrieved November 11th 2013. <http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea>

[55] Eun-Jung, Kim: "S. Korea military to prepare with U.S. for cyber warfare scenarios". Yonhap News Agency on April 1st 2013. Retrieved November 3rd 2013. <http://english.yonhapnews.co.kr/national /2013/04/01/20/0301000000AEN20130401004000315F.HTML>

the proportionality or likelihood of success principles. However, the application of principle of Just War Theory will demonstrate whether the U.S. and South Korea are justified in retaliating using cyberweapons and why such a response may avoid any nuclear confrontation between the U.S. and the DPRK.

Consider the principles of jus ad bellum and how they may be applied to this case. North Korea has used cyberweapons against South Korea while the two countries are technically at war and after making repeated statements of its intent. It has also threatened to use nuclear weapons to strike at both the United States and South Korea and made active efforts to develop long-range missiles to deliver the nuclear payload for this very purpose. It is clear from the very onset that the United States and South Korea have just cause to deploy cyberweapons against North Korea in this scenario. This would be in response to attacks made by North Korea since the U.S. would be acting in defense of its ally, South Korea. The just cause principle allows a country to enter into war, or in this case, a cyber war, in defense of others that have been recently attacked and therefore, be satisfied in this situation.

The U.S. has already invested in an extensive cyberweapons program and leaked documents have shown that such investments are a fraction of the cost of any conventional military action taken by the U.S. in the past. The costs of using cyberweapons against the DPRK's military infrastructure would be greatly outweighed by the benefits of the protection to South Korean cyberspace as well as U.S. cyber interests in the region. The principle of proportionality which takes into account the costs and benefits of any entering any war would certainly be satisfied in this case. Intelligence reports from South Korea suggest that the DPRK has about 3,000 hackers that are a part of different cyber strike teams. This pales in comparison to the resources and sophistication of the U.S. cyberweapons program that was responsible for

damaging and delaying Iran's nuclear program. Thus, it is highly probable that the U.S. would prevail in any cyberwar situation against North Korea. It is also important to consider reasons why using cyberweapons may once again be permissible under the Just War doctrine as opposed to conventional or even nuclear weapons. As North Korea and the U.S. both possess nuclear weapons with long-range capabilities, a nuclear-war situation would assure mutual destruction and not be a success by any standard. The use of cyberweapons to cripple North Korean cyberwarfare capability would secure South Korean cyberspace and prevent the DPRK from using cyberweapons as a way to assert dominance on the Korean peninsula. Indeed, using this case as an example, one could claim that in any conflict situation between two nuclear-armed states, the only recourse would be the covert use of cyberweapons as any open invasion would trigger the use of nuclear weapons and result in mutually assured destruction for both sides.

The remaining principles of jus ad bellum that must be taken into consideration are right intentions, legitimate authority, and last resort. First, it is evident that any retaliatory response by the U.S. and South Korea would satisfy the right intentions principle, as the response would not seek to make territorial gains in the Korean peninsula. The object of any cyberattack would be to nullify the threat of North Korean cyberweapons and safeguard the interests of the citizens of South Korea by protecting their cyberspace. Second, the principle of legitimate authority would be satisfied as any action involving the cyberweapons program by the U.S. would have to be authorized directly by the President, Barack Obama. The case would be similar if South Korea was to engage in any hostile cyberwarfare action but the likelihood of the U.S. responding to North Korean cyberattacks is far greater in this situation. Third, any retaliatory cyberattack by the U.S. would be justified in this situation as the last resort principle has limited applicability in the case of conflicts where one side has already been attacked. It is evident that when one side is

already engaging in warfare, diplomacy or attempts at negotiation would not serve much of a purpose. Thus, under the principles of jus ad bellum, the U.S. and South Korea would be justified in attacking North Korea with cyberweapons, but not conventional weapons.

The principles of the second tenet of Just War Theory, jus in bello, concern matters of proportional response and discrimination between targets during campaigns in a war. As we know, North Korea's cyberattacks on South Korean's infrastructure affected over 30,000 computers in the country and have so far cost the country over 800 million U.S. dollars. A proportional response by the U.S. to defend its ally would unquestionably justified in this situation. However, it is important to state that while cyberattacks by North Korea have violated the principle of discrimination by damaging civilian infrastructure and causing harm to civilians in Seoul and other South Korean territories, the U.S. must only target the DPRK's military operations. The principle of proportionality can also be used to reinforce the argument that the U.S. and South Korea would only be justified in the use of cyberweapons and not conventional weapons that could result in the loss of human lives. This is because while North Korea's attack did damage civilian infrastructure, no deaths have been attributed to the attacks.

While the principle of discrimination was violated by the DPRK, the Just War doctrine does not allow for a state to commit the same violation as another when engaging in war. This is logical considering if such violations were allowed, all manner of justice in warfare would disintegrate with the introduction of simply one unjust party. There are concerns that any cyberattack by the U.S. could go rogue, as was the case with the Stuxnet virus used against Iran, and cause damage to civilian infrastructure. However, reports suggest that the U.S. was able to learn from the mistake of letting a virus go uncontrolled and has taken steps to build better controlled viruses for future use. Furthermore, most of the cyberspace in North Korea is state

owned and controlled and as such any cyberattack would almost certainly only affect military and state infrastructure. Thus, it is highly unlikely that the U.S. would violate the principle of discrimination by using cyberweapons against North Korea.

This is perhaps the most clear case of a situation where Just War Theory may be applied to a cyberwar and determine if the actions of the states involved are just or not. While proponents of cyberwarfare do not usually provide an ethical basis for the use of cyberweapons, the application of the Just War doctrine to this situation shows that Just War Theory can be applied and is useful to determine the ethics of actions taken by states in the cyberspace. Indeed, not only is Just War Theory used to determine if North Korea's actions were just, but it also provides ethical basis for retaliatory action by the United States and South Korea.

CONCLUSION

The increased global focus on cyberwarfare should not come as a surprise to anyone who has been following the news for the last decade. All the major world powers including the United States and China have invested heavily into cyberweapons programs and cybersecurity in order to gain an edge in this new arena of war. Modern weapons and military infrastructure rely heavily on systems that can be targeted by cyberweapons and the rise in the reliance of these systems has corresponded to an increase in cyberterrorism by groups such as Anonymous globally. Almost every conflict situation involving the United States today has an element of cyberwarfare and understanding the ethics of cyberwarfare has become the focus of many military ethicists such as Randall R. Dipert and Colonel James Cook.

The cases discussed in this paper demonstrate that cyberwarfare need not be treated any differently from conventional warfare from an ethical perspective. While cyberwarfare is conducted differently, has unique features, and may have different results – the intentions and objectives of entities using cyberwarfare remain the same. As has been the case with Just War Theory in the past, there are many proponents as well as detractors of the doctrine's applicability in the age of cyberwarfare. While international laws and U.N. conventions may not be suitably applied to cases of cyberwarfare due to their specificity, the application of the broad principles of Just War Theory presents no such problems. This is because Just War Theory deals with the intents and effects of warfare, regardless of the type of warfare in a situation. It may be the case that Just War Theory needs to be modified to accommodate other advancements in weaponry that render it inapplicable in the future, but the advent of cyberweapons does not require any such modifications yet.

BIBLIOGRAPHY

1. Dipert, Randall R.: "The Ethics of Cyberwarfare." Journal of Military Ethics Volume 9, No. 4. Published by Routledge in 2010.

2. Cook, James: " 'Cyberation' and Just War Doctrine: A Response to Randall Dipert". Journal of Military Ethics Volume 9, No. 4. Published by Routledge in 2010.

3. Nguyen, Reese: "Navigating Jus Ad Bellum in the Age of Cyber Warfare". California Law Review, Volume 101: 1079. Published in 2013.

4. Shoamanesh, Sam: "History Brief: Timeline of US-Iran Relations Until the Obama Administration". MIT International Review: http://web.mit.edu/mitir/2009/online/us-iran-2.pdf

5. Katzman, Kenneth: Iran: U.S. Concerns and Policy Responses. Congressional Research Service on 5th September 2012.

6. Majd, Hooman: *The Ayatollah Begs to Differ: The Paradox of Modern Iran*. Published by Doubleday NY in 2008.

7. Libicki, Martin C.: "A matter of Degree: Who Can Authorize a Cyberattack?." Federation of American Scientists on January 9th 2013: http://www.rand.org/commentary/2013/01/09/FAS.html

8. Fotion, Nicholas: "War & Ethics: A New Just War Theory". Continuum International Publishing 2007.

9. United States Department of States, Office of the Coordinator for Counterterrorism: "Country Reports on Terrorism 2009": http://www.state.gov/documents/organization/141114.pdf

10. Fletcher, Holly: "State Sponsor: Syria". Council on Foreign Relations in February 2008. Retrieved on November 13th 2013: http://www.cfr.org/syria/state-sponsor-syria/p9368

11. Boxx, Lt. Colonel Edward S., USAF: "Observations on the Air War in Syria". Washington Institute, March–April 2013: http://www.washingtoninstitute.org/uploads/Documents/opeds/Boxx20130301-AirSpace.pdf

12. Selden, Mark and So, Alvin: “War and State Terrorism: The United States, Japan, and the Asia-Pacific in the long Twentieth Century”. Published by Rowman & Littlefield in 2003.

13. Department of Defense: “Military and Security Developments involving The Democratic People’s Republic of Korea”. Annual Report to Congress 2013. http://www.defense.gov/pubs/report_to_congress_on_military_and_security_developments_involving_the_dprk.pdf