WHAT CONSTITUTES AN ACT OF WAR IN CYBERSPACE?

THESIS

Kelli Kinley, Captain, USAF

AFIT/GIR/ENV/08-M12

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/08-M12

WHAT CONSTITUTES AN ACT OF WAR IN CYBERSPACE?

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Kelli Kinley, Captain, USAF

March 2008

AFIT/GIR/ENV/08-M12

WHAT CONSTITUTES AN ACT OF WAR IN CYBERSPACE?

Kelli Kinley, Captain, USAF

Approved:

//SIGNED//	25 Mar 08
Dr. Dennis Strouble (Chairman)	Date
//SIGNED//	25 Mar 08
Dr. Michael Grimaila (Member)	Date

Abstract

In December 2005 a new mission statement was released by the Air Force Leadership, “to deliver sovereign options for the defense of the United States of America and its global interests...to fly and fight in Air, Space and Cyberspace.” (Wynne & Mosley, 2005) With the stand up of the AFCYBER command and the use of cyberspace to carry out our daily mission the USAF needs to have a clear understanding of what war in cyberspace looks like and what the laws are governing war in cyberspace. This research and it’s resulting data analysis is intended to provide a better understanding of what the current laws of war are and how they translate to cyber war and the complexities that exist, along with recommendation on future revisions of the laws.

Acknowledgments

I would like to thank Dr. Dennis Strouble for his guidance and boundless support throughout the course of this thesis effort. I appreciate your patience, continuous support, and positive attitude through from finding a thesis topic to the conclusion of this research. Your support and undivided attention were key to helping me narrow down my topic and understanding the laws that apply. To Dr. Michael Grimaila, your insight and recommendations were invaluable in ensuring the results of this thesis were complete and professionally summarized.

In addition, I would like to thank my daughter for keeping a good attitude and understanding sometimes I had to just have some time to my self to type. My hope is that she will take a lesson from this process and see that hard work, diligence and great attitude does pay off at any age.

Kelli Kinley

Table of Contents

Page

List of Tables

Page

WHAT CONSTITUTES AN ACT OF WAR IN CYBERSPACE?

". . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."

Sun Tzu, The Art of War

I. Introduction

Background

In a background report from the Pentagon, December 1999, top pentagon officials stated that the United States was in a virtual war in cyberspace. It stated that the United States of America was being "invaded," every hour of every day, by hostile forces using computers. (Randle, 1999) Since this report, many researchers have stated that cyber warfare is tempting for our adversaries because our military forces are so over whelming it makes conventional attacks less likely. Instead of fighting with high cost of fighter aircraft, tanks, or bombs, anyone with access to a computer and the internet can cause grave damage.

In December 2005 a new mission statement was release by Air Force Leadership, "to deliver sovereign options for the defense of the United States of America and its global interests…to fly and fight in Air, Space, and cyberspace." (Wynne & Mosley, 2005) The newest major command of the U.S. Air Force is the Air Force Cyberspace Command (AFCYBER) which is expected to be in full capability by October 2009. Major Gen William Lord will be the first commander and he summarizes the mission as:

"The aim is to develop a major command that stands alongside Air Force Space Command and Air Force Combat Command as the provider of forces that the President, combatant commanders and the American people can rely on for preserving the freedom of access and commerce, in air, space and now cyberspace."

With this formal acknowledgement of cyberspace a domain in which the military can and will wage war it brings with it challenges and questions. One of the biggest challenges of the new command will be clarifying or defining what is an act of war in cyberspace.

Over the decades the way the U.S. militaries communicate and fight has changed drastically. Relying more on computers and the infrastructure needed to carry out our day to day lives. (Wynne & Mosley, 2005) Our nations critical infrastructure consists of the physical and cyber assets owned and operated by public and private companies that control our critical support structures (i.e. agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous material and postal and shipping to name a few). As stated in the National Strategy to Secure Cyberspace, February 2003, cyberspace is the nervous system of our country and our national security is depending on our ability to secure cyberspace.

In spring of 2007, Estonia claimed to be under attack, not in the traditional sense by guns or bombs, but in the form of data request from more than a million computers. This attack overwhelmed the nation's computer networks, crashing e-mail for its

parliament, taking down emergency phone lines and freezing online services of government offices, banks, universities and hospitals. Estonia accused Russia of conducting a "cyber war" in retaliation for a decision to move a Soviet-era war memorial. The Russian government denied involvement. (Hollis, 2007) However, 2 May 2007 Estonia opened a criminal investigation under the Estonian Penal Code criminalizing computer sabotage and interference with the working of a computer network. Estonia investigated the incident and was able to track the attack back to the Kremlin. However, it is not known if the attack actually came from the building or if a zombie computer was used from this building. They were unable to tell if the person who launched the attack was affiliated with the government or if they were a civilian acting on their own.

As the world grows more dependent on computers, internet and cyberspace it is evident it is a pool of information that is constantly being updated, expanded and growing. You can find anything on the internet, including how to build bombs, launch a denial of service attacks and basic hacker tutorials. In March 2007, researchers at the Department of Energy's Idaho National Laboratory conducted an experimental cyber attack and managed to make a generator self-destruct. (Hollis, 2007) Computer attacks don't just threaten other computers but the larger infrastructure that controls vital resources. Viruses could become as dangerous as missiles. At the same time, cyber attacks offer militaries the option of disabling an enemy's vital infrastructure temporarily or completely destroying it. (Hollis, 2007) They are able to hinder their daily operations and perhaps stop further attacks without firing a traditional weapon.

Research shows cyberspace is the new battleground. The U.S. needs to learn when and how to deploy weapons against our enemy without physical battle if appropriate. What are the rules of cyber war? (Hollis, 2007) When should an act in cyber war translate and give just cause for actual physical war?

Problem Statement

Serious "interpretation" would have to take place in order to convert current laws, treaties, torts that would also fit into the cyberspace and cyber war. An example, the U.N. Charter, "clearly prohibits states from using force except in self defense or with U.N. authorization." (Hollis, 2007) What does this mean for situations such as, the Estonia Russia computer attacks? Is it only considered use of force if they would physically break into the parliament or other government building? Even though the computer attack was not a traditional "physical" attack, they perpetrator did however, physically enter the computers of the parliament and cause damage. In the absence of laws of war, then the exiting laws are construed to make them fit into more complex international and foreign laws. Such as, if the hackers in the Estonia case were indeed identified as living in and launching the attack from Russia, but had no ties to the government or military. Under existing rules, Estonia should have respond by asking Russia to police its own territory. (Hollis, 2007) If Estonia would have launched an attack at Russian it would have breached Russia's sovereignty. As Duncan Hollis wrote in his article, E-war Rules of Engagement, nations could agree to waive sovereignty and permit a direct response in cyber attacks by terrorists that all nations might want.

However, Estonia was able to track the attacker and arrested him. He was and ethnic Russian living in Estonia. Estonia is still investigating if the attacker was working alone or with a group. (Fox News, 2008)

Based on the background provided, the following problem is addressed in this thesis: What constitutes an Act of War in Cyberspace? With the stand up of the AFCYBER command and the use of cyberspace in our daily mission the USAF needs to have a clear understanding of war in Cyberspace. In the next few chapters the data will define cyberspace, information ware-fare, some actors, Law of Armed Conflict (LOAC), Geneva Convention, Weapons of Mass Destruction (WMD), The Outer Space Treaty and what is missing from current laws. Nations have devised rules of international law, such as the Geneva Convention, Laws of Armed Conflict, which seek to avoid war or minimize human suffering when conflicts occur. As new technologies emerge, leadership needs to draft new rules by which to fight in cyber war. So far, there have not been any changes to international law in order to govern attacks on or by computers and reason for this is that many feel current laws convey to cyberspace. (Hollis, 2007)

Limitations

The first limitation on this thesis was the lack of material and experts to draw from on the subject. The concept of cyber war is not necessarily new. Many scientists and top level leaders in the country and around the world have been envisioning the concept of cyber war for decades. However, until recently, with the official stand up of the AFCYBER Command, cyber operations are new to the military are a work in

progress, few decisions are complete. Since experts in the field of cyber war are still undetermined, it was necessary to infer who the experts will likely be and what acts in cyber war are considered an act of war from documents, policy, international laws, treaties and other similar resources.

Another limitation for this thesis was the lack of official documentation on cyber war and what is considered an act of war and how the U.S. will respond. There have been several cyber war attacks against the United States and other countries, but there's no documentation on how to respond. The number of articles and legal documentation on when to respond in self defense, attribution and to counter an attack are limited.

Scope

Considering what is considered and act of war and the scope of cyber war are too expansive to discuss in one thesis. For the purpose of this thesis the research used will look at cyberspace and the laws governing war in cyberspace. Since the advent of cyberspace is new and fighting in cyberspace is relatively new, there have not been any new international laws, torts or treaties to convey to cyberspace. The research for this thesis pertains to current laws and how they apply to cyber war. Therefore, this research provides a foundation for further research and development of new cyber war laws.

II. Literature Review

Introduction

This chapter summarizes the literature reviewed to understand the research problem and support the proposed proposition. First, this chapter provides background information that will enable the reader to understand key research concepts related to the complexity of cyber war and what constitutes an act of war in cyberspace. This will be accomplished by defining what is considered cyberspace and what is considered an act of war in cyberspace and how information warfare fits in. Next, a review of the Laws of Armed Conflict (LOAC), Geneva Convention, United Nations Charter, and the Outer Space Treaty and Telecommunications Act. Along with defining theses laws they are followed by examples of ways they may be translated into cyber warfare. This section provides the preponderance of data used for the content analysis. Finally, as discussed in the Harvard Review article it is especially important to obtain attribution in cyber warfare. Unlike traditional warfare, cyber warfare is much more difficult to establish who conducted the attack and their intent. With attribution in a cyber attack it can be decided what laws apply, and how to proceed with a counter attack. The laws that apply and how the U.S. responds to an attack is determined by who launched the attack and if they are working for a government or not. The intent of this section is to provide some insight into how U.S. militaries may conduct counter attacks and how international laws apply. Altogether these three sections will determine what cyber war is and how current laws translate or not.

Defining Cyberspace

Cyberspace

Cyberspace is defined in the Air Force Core Concepts as a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. Cyberspace exists across the other physical domains of air, land, sea, and space and can facilitate contact between the cognitive processes and the physical domains. (8TH AFCC, 2007) In short, cyberspace exists when someone builds and operates networked electronic systems that send or receive data using electromagnetic energy. (8TH AFCC, 2007) With this in mind, there are adversaries that do not possess robust cyberspace capabilities but are able to challenge the United States using third party systems. They may use zombie computers, and this becomes an added consideration when responding to an attack.

The breadth of cyberspace involves components that operate across all other domains to include internet protocol (IP) based terrestrial, airborne and space networks, non-IP based networks and data links, telephone networks, and control systems. Electronic attack, directed energy and electronic protection are examples of capabilities that can be used to create effects in and through cyberspace. (8TH AFCC, 2007)

War fighting in Cyberspace

Currently, all the U.S. services and many national agencies maintain capabilities that use particular aspects of cyberspace to accomplish their specific missions. For example, intelligence organizations, which are collecting and analyzing data, use network

capabilities to exploit the Global Information Grid and associated network infrastructures for foreign intelligence and counterintelligence purposes. (8TH AFCC, 2007) Force protection units use frequency jammers to counter improvised explosive devices (IEDs) or high powered microwave (HPM) to control crowds in an urban environment. These types of operations represent different ways that cyberspace is used, but not how the domain itself is controlled. (8TH AFCC, 2007)

The war fighter's first priority is to ensure friendly use of cyberspace while denying that same use to the adversary. (8TH AFCC, 2007) A whole domain perspective also recognizes that cyber capabilities can be used to synchronize and integrate combat operations across the other domains. War fighting in cyberspace basically means countering our adversary capabilities through our attacks on his systems while defeating any attempts to counter our use of cyberspace. This is an immense far reaching mission that goes far beyond networks, servers and personal computers. (8TH AFCC, 2007) There are three categories of war fighting operations in cyberspace: ensuring operational freedom of action; delivering cross domain effects; and, supporting civil operations. (8TH AFCC, 2007)

Information Warfare

The information age is here and it's going to continue to grow. The scope of information warfare has, embraces every aspect of information use that would permit war without battle. (Dicenso, 1999) This includes human intelligence (HUMINT), electronic intelligence (ELINT), communications intelligence (COMINT), psychological operations (PSYOP), and every other method of gathering and affecting information that may be used to the advantage of one nation or to the detriment of another during a conflict. (Dicenso, 1999) On a daily basis, computers, software, e-mail and the world-wide web

continue to have a dramatic impact on how the U.S. sees war and how they view what is considered war. As discussed in the article by Mark Shulman, Air War College, the effect technology has had is to change not only the battlefield, how our militaries fight our adversaries, the actors and the types of targets selected, will ultimately, change the rules of military operations, as seen with the stand up of the Cyberspace Command. Advances in all technology, including military technology, have out-paced changes in the laws governing how the U.S. fights war in cyberspace. (Shulman, 1999) Over the past decade, the fastest developing type of "armed conflict" is IW. Ironically, IW is neither “armed,” nor does it necessarily involve “conflict.” (Shulman, 1999) For instance, Special Forces detonate a small non-nuclear electromagnetic pulse weapon near a nation's central bank computer storage facility, destroying the electronic systems that transact, communicate, and archive the nation's financial information. What if, communication specialists tapped into another state's television broadcast "morphed" images of that state's religious leader engaged in sacrilegious acts? Or, another communications specialist hacks into a target nation's computer network coordinating air or rail traffic to reprogram the systems to shut down without warning. (Shulman, 1999) Each of these hypothetical examples would cause severe damage to the nations involved: economies could be destroyed; governments would fall; planes and trains crash. Thousands of people would perish. As dramatic as these hypothetical’s are, they demonstrate how complicated IW is and just how devastating it can be. (Shulman, 1999) What makes it even more complicated is that if done correctly, the attacks go undetected.

The Air Force appears to be the lead agency in studying IW, for the purpose of this thesis their definition will be used: IW is any "action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions. (8TH AFCC, 2007) It includes electronic warfare, military deception, physical destruction, security measures, and information attack. (8TH AFCC, 2007) The Air Force defines information as "data and instructions" and distinguishes IW from warfare in the information age as attempts to influence information directly.

Defining Laws and how they translates to cyber war

Laws of Armed Conflict

The LOAC exists from a desire between civilized nations to prevent unnecessary suffering and destruction, while keeping the effective of waging war. LOAC is part of international law, and regulates the conduct of armed conflict. Its main purpose is to protect civilians, prisoners of war, the wounded, sick, and shipwrecked. LOAC applies to international armed conflicts and in the conduct of military operations and related activities in armed conflict. (Powers, 2006) Also, closely associated with LOAC is the Hague Convention on Land Warfare and requires that all necessary steps must be taken to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided that they are not being used at the time for military purposes. (Hague Convention, 1954) Therefore, since LOAC covers the laws of war, the Hague Convention covers aspects

regarding protection of marked buildings then it is easy to recognized how these two laws correspond to one another.

There are currently four important LOAC principles governing armed conflict—military necessity, distinction, proportionality and chivalry.

Military Necessity. Military necessity is what it sounds like. It requires military forces to engage only in those acts necessary to accomplish a legitimate military objective. Attacks are limited strictly to military objectives. In applying military necessity to targeting, the rule generally means the U.S. military may target those facilities, equipment, and forces which, if destroyed, would lead as quickly as possible to the enemy's submission. (Brown, 2006)

Military necessity also applies to weapons review. AFI 51-402, Weapons Review, requires the Air Force to perform a legal review of all weapons and weapons systems intended to meet a military requirement. These reviews ensure the U.S. complies with its international obligations relating to LOAC, and it helps military planners ensure military personnel do not use weapons or weapons systems that violate international law. Some examples of illegal arms for combat include poison weapons and expanding hollow point bullets. (Brown, 2006)

Distinction. Distinction is basically discriminating between lawful combatant targets and noncombatant targets, such as, civilians, civilian property, POWs, and wounded personnel out of combat. Distinction means military missions, only engage valid military targets. An indiscriminate attack is one that strikes military objectives and

civilians or civilian objects without distinction. Distinction requires defenders to separate military objects from civilian objects to the maximum extent feasible. Therefore, it would be inappropriate to locate a hospital or POW camp next to an ammunition factory. (Brown, 2006)

Proportionality. Proportionality prohibits the use of any kind or degree of force that exceeds that needed to accomplish the military objective. Proportionality compares the military advantage gained to the harm inflicted while gaining this advantage. Proportionality requires a balance between a direct military advantage anticipated by attacking a legitimate military target and the expected incidental civilian injury or damage. Proportionality seeks to prevent an attack in situations where civilian casualties would clearly outweigh any military gains. This principle encourages combat forces to minimize collateral damage. (Brown, 2006)

Geneva Convention

The Geneva Convention of 1949 was basically derived from instances that occurred during the two World Wars and it is the base of the current LOAC. The Geneva Convention consists of four treaties that set the standard for international law for humanitarian concerns. The main concern is the treatment of non-combatants and prisoners of war. They do not affect the use of weapons in war, which are covered by The Hague Conventions of 1899 and 1907 and the Geneva Protocol on the use of gas and biological weapons of 1925. The first convention was signed in Geneva Switzerland in 1864 and it covered the sick and wounded in war and it was expanded on in 1906. Two

more conventions covering the wounded and prisoners of war were signed in 1929. Again, in 1949 four new conventions were signed, the primary one being the treatment of civilians during wartime. (World Almanac and Book of Facts, 2008) The treatment of civilian's convention of 1949 provided safeguards for wounded civilians, children under 15 years of age, pregnant women, and the elderly. It also forbids the use of discrimination based on racial, religious, national or political grounds. This same convention also specifies torture, collective punishment, reprisals, unwarranted destruction of property, and that the civilians cannot be used by the armed forces while captive. Civilians are to be treated humanely, fed adequately and have access to supplies needed and are not to be forced to disclose more information than what is common knowledge. (World Almanac and Book of Facts, 2008)

Cyber warfare is making it difficult to distinguish between military and civilian targets since ninety percent of the United States current infrastructure is privately owned and operated. (Brown, 2006) This being the case it blurs the line and makes it even more difficult to distinguishing legitimate targets within our critical infrastructure. The 1977 Protocol I to the Geneva Conventions established the "Basic Rule" on discrimination which is more difficult to apply to cyber war. (Shulman, 1999) In order to ensure respect for and protection of the civilian population and civilian objects, conflicts have to distinguish between the civilian population and combatants and also between civilian objects and military objectives and only direct operations toward the military objectives. (Shulman, 1999)

Article 51 protects civilian populations and defines unlawfully indiscriminate attacks: (a) Not directed at a specific military objective; (b) which cannot be directed to a specific military objective; or (c) which cannot be limited as required by this Protocol; and in each case, are of a nature to strike military objectives and civilians without distinction. (Shulman, 1999)

Traditional tools for distinguishing civilian from military personnel are not as black and whit as they were before long-range bombardment and telecommunications. Traditionally for combatants wore uniforms that visibly distinguished them from noncombatants. Likewise, most warfare involved physical proximity. No matter what the weapon, a sword or a projectile, most combatants could see each other and distinguish combatants from noncombatants. One exception was aerial bombardment by airplane or missile. Even then however, airmen doing the targeting still had to make realistic distinctions. With Cyber war it is inconsequential whether they are wearing military uniforms or not. For example, someone launching a computer virus to attack an American military communications system may be sitting in a basement of a public building wearing a doctor scrubs or a clergy robe. Instead of a military uniform, he would be wearing the symbol of the medic or clergy, which by traditional warfare are protected. He could be part of a protected group sitting in a privately-owned building. This example shows how cyber war may not be a physical proximity to distinguishing combatants from non-combatants. Therefore, in regards to causing damage and destruction of a vital computer or LAN this individual could be seen as a combatant and subject to proportional response. (Shulman, 1999)

The USAF believes the correct formula for an attack must be likely to produce a military advantage that outweighs civilian casualties and damage. (Shulman, 1999) In order to do this the USAF must weigh the importance of navigation systems, communications systems, and electrical grid systems to the opponent's military effort. Should the advantage be measured in lives saved or lost; dollars spared saved, risked; or only in permanent physical destruction? IW affords us opportunities that traditional conventional weapons do not; degrading a system could be reversible in ways that physical destruction could not. This translates to lives saved whereas systems become inoperative either permanently or briefly. Does this therefore mean that reversible attacks will be launched against civilians or civilian infrastructure more freely? Maybe. Does it strengthen adherence to the norms of discrimination? If the goal is to protect civilian lifestyles as much as possible during the operation, then the answer is "no." If the aim is to contain war's destructiveness and to facilitate restoration of civil society after the conflict, then the answer is "quite probably yes." (Shulman, 1999)

Weapons of Mass Destruction

As defined by the Department of Defense Weapons of Mass Destruction (WMD) are weapons that are very capable of high destruction and of being used to destroy a large number of people. Generally WMDs are high damage causing explosives or nuclear, biological, chemical and radiological weapons. (DTIC, 2008)

AF Handbook 10-2502, USAF Weapons of Mass Destruction Threat Planning and Response handbook, states terrorist use of chemical and biological weapons within the United States is a Federal offense under Title 18. U.S. Code (USC) Section 175 for biological weapons possession and Section 229 for chemical or biological

weapons use as a WMD. (AFH 10-2502, 2001) Even when conducted overseas, any property owned, leased or used by any US agency or department, having a chemical or biological weapons attack is a Federal offense, Title 18 USC, Section 229(4).

AF Handbook 10-2502, USAF Weapons of Mass Destruction Threat Planning and Response handbook, also covers the use of WMD during wartime between nations. It sates that the use of chemical or biological weapons from on nation to against another nation is a clear violation of LOAC.

Per DoDD 5100.77, paragraph 5.6, the U.S. Army is the DoD Executive Agent for LOAC violation issues and they are responsible for performing investigations pertaining to chemical and biological weapons.

However, none of the directives listed above, nor LOAC defines a WMD in cyberspace. My research however, introduced WMD in cyberspace and requires attention. Some examples WMD in cyberspace are, if an attacker where to target a dam and open up the flood gates electronically. This could cause a massive amount of deaths depending on what dam they were to attack. Or, if an attacker were to use cyberspace to hack into a power grid and take out power to a large area of the U.S. An attack of this type would affect everything from electricity, to transportation and medical facilities. An attack of this magnitude could cause thousands of deaths, not to mention injuries and trauma. Examples like these have been used in sci-fi books and movies since the 1970's, but have not been look at seriously lawmakers that affect LOAC, U.N. Charter and other international laws. Currently, attacks by terrorist or terrorist groups are considered a criminal act in the country from which it occurred but does not fall under a LOAC

violation. Therefore, if an attack was carried out from a foreign country the U.S. would have no recourse at this time unless the hosting country would be willing to prosecute the accused.

The Outer Space Treaty

It was not very long ago, when thoughts of preserving space for peaceful purposes began at the United Nations in the 1950's. In 1957 the U.S. and its allies submitted their proposals for how the treaty should look for reserving space exclusively for "peaceful and scientific purposes," (Ruseck, 2003) but the Soviet Union rejected all proposals based on their preparation to launch the world's first satellite and in order to test its first intercontinental ballistic missile.

The U.N. resolution of 1884 called on countries to refrain from stationing WMDs in outer space. U.N. resolution 1962 set legal principles on outer space exploration, stipulating that all countries have the right to explore space. In 1963, these two resolutions became the framework for the Outer Space Treaty. The U.S. and the Soviet Union submitted two separate proposals in 1966. After review both, they came up with a mutually agreed proposal and it was agreed upon and approved on December 19, 1966 and was signed and approved by all parties and entered into force October 10, 1967. (Ruseck, 2003)

Basically the Outer Space Treaty of 1967 bans stationing WMDs in outer space, spells out the legally binding rules of space exploration, and prohibits military activities on celestial bodies. Ninety-seven countries are part of the treaty; North Korea is the only state with real potential for space-launch capabilities that has not signed the

treaty. Many countries seem to be concerned with the U.S. missile defense plans and space policy. China has proposed a disarmament agreement in Geneva in the hopes to negotiate a treaty in order to prevent and arms race in outer space. The U.S. insists there is no need for the treaty, because at this time there is not an arms race for outer space.

The basic treaty terms forbid countries from deploying "nuclear weapons or any other kind of weapons of mass destruction" in outer space. In the treaty the definition of WMD is not spelled out, but is to be commonly understood as nuclear, chemical, and biological weapons. One thing the treaty doesn't address is the launching of ballistic missiles, which could be armed with nuclear warheads through space. The treaty emphasizes that space is used for peaceful purposes which could be interpreted as all weapons through space.

The treaty's key arms control provisions are in Article IV, parties commit not to:

- Place in orbit around the Earth or other celestial bodies any nuclear weapons or objects carrying WMD
- Install WMD on celestial bodies or station WMD in outer space in any other manner
- Establish military bases or installations, test "any type of weapons," or conduct military exercises on the moon and other celestial bodies other treaty provisions underscore that space is no single country's domain and that all countries have a right to explore it.

These provisions state that:

- Space should be accessible to all countries and can be

- Space and celestial bodies are exempt from national claims of ownership
- Countries are to avoid contaminating and harming space or celestial bodies
- Countries exploring space are responsible and liable for any damage they cause
- Space exploration is to be guided by "principles of cooperation and mutual assistance," such as obliging astronauts to provide aid to one another if needed (Ruseck, 2003)

As stated above, the Outer Space Treaty prohibits nations from stationing WMD on a celestial body. However, it does not cover weapons moving through outer space, such as, Nuclear weapons on a missile. It addresses space as a peaceful place. There are currently satellites in space that aid in our daily lives, such as, telecommunications and global positioning systems (GPS). It could be argued, that if an attacker were to target a satellite it could be used as a WMD. For example, if an attacker were to shut off a satellite that controls GPS. With the amount of airlines, military operations and transportation systems world-wide that would be affected by this could be catastrophic. Again, a weapon of mass destruction is not really defined, other than traditional thinking of chemical, biological weapons. However, as the name states, Weapon of "Mass" Destruction, how many lives is considered "Mass." Current laws do not define how many people have to be killed, injured or affected by an attack to be a WMD.

International Maritime Satellite

International Maritime Satellite (INMARSAT) as stated in AMC Instruction 33-109, International Maritime Satellite Management, is a commercial comm. System subject to international law and treaty. It is a radio comm. device using a satellite link to interface with terrestrial telephone systems or other mobile terminals. Terminals are commissioned as land, air or sea terminal. Once commissioned, the terminals may be used only in the configuration stated in the commissioning application. (DiCenso, 1999)

There are 79 countries on the international INMARSAT treaty. One of the provisions of the treaty is that it may only be used for administrative, humanitarian and peacetime applications or under the auspices of the United States. The system may not be used for making war or for example it cannot be used to direct air strikes etc. (DiCenso, 1999)

Defense Information Systems Agency (DISA) and Defense Information Technology Contracting Organization (DITCO) consider INMARSAT long-haul telecommunications systems per Department of Defense Instruction 46410-14, Base and Long-Haul Telecommunications Equipment and Services. (DiCenso, 1999)

Attribution

Actors

The United States has routinely conducted surveillance flights over China in order to gain electronic and visual intelligence. The Chinese government was aware of it and began sending jet fighters to accompany, our reconnaissance planes. On 1 April 2001 an American surveillance plane collided with a Chinese fighter about seventy miles off the

coast of China. The American plane had to make an emergency landing in China. The Chinese jet spun out of control and was lost at sea killing the pilot Wang Wei. (Creekman, 2002)

Both countries blamed each other for the incident. (Creekman, 2002) Word spread, and some American citizens were angry over the accusations China was making. Armed with the internet, they stated trash talking over the internet and they managed to deface and vandalize at least sixty-five Chinese websites. (Creekman, 2002)

In retaliation, a group of Chinese hackers, calling themselves the "Hackers Union of China," declared war on America. (Creekman, 2002) The Hackers Union of China declared the week of 1 – 7 May 2001 as "Hack the USA" week they took credit for shutting down or altering multiple U.S. government websites, including the websites for the Office of the Clerk of the United States House of Representatives and the White House. The hackers replaced the content of one site with China's fluttering red flag and rendition of the Chinese national anthem that automatically played whenever users accessed the site. (Creekman, 2002) Hackers replaced other sites with tributes to downed Chinese pilot, Wang Wei or plastered the sites with messages such as "Beat down Imperialism of American" and other anti-American, pro-Chinese sentiments. The hackers ended their war after claiming to have hacked one thousand American websites. However, it has been speculated, that the Chinese government was actually responsible for the attack not just a renegade hacker club. (Green, 2002)

Computer hacking is becoming more widespread and does not entail the person having a degree in computer engineering or computer science. Anyone with access to a

computer and the internet can find step-by-step hacking tutorials and can begin when and where they like. Hacking into another computer is considered trespassing in the United States and carries its own punishments under the Computer Fraud and Abuse Act (CFAA); most experts are more worried about the damage the hacker can cause after gaining access, rather than the hack itself. (Creekman, 2002)

Hackers – Non-vital target

If a citizen of another nation where to become a hacker and spread a virus that would erase all files on an infected computer, and that virus were to spread throughout the US, infecting fifty percent of the nation's personal computers, believe it or not there are not very many if any legal recourses available to the victims. If this same hacker was an American citizen-hacker and spread the same virus throughout the U.S. it would be near impossible to prosecute. But if this hacker is from another country and there was not an extradition treaty with that country then the odds of this hacker finding his way into a U.S. court room would be even more astronomical.

The most difficult tasks would be to bring a citizen hacker from another nation to the U.S. to face trial. In an earlier case, factor v. Laubenheimer, the Supreme Court held that the legal right for a country to demand extradition of another country's citizen exists only when it is created by treaty. (Creekman, 2002) Because the U.S. does not usually enter into treaties with countries, there is no extradition treaty with other nations, and thus, no legal ground to demand the extradition of a citizen hacker to face an American judge. The U.S. could conceivably ask for extradition absent a treaty, the U.S. inability to comply with the reciprocity for which the other nation would undoubtedly ask, would probably mean the other nation would deny the request. (Creekman, 2002)

Another possible way to bring a citizen hacker to justice in the U.S. is through extralegal seizure. In U.S. v. Alverez-Machain, the Supreme Court held that a federal court did not lose jurisdiction over a suspect because that suspect had been abducted from Mexico and brought to the U.S. for trial without resorting to the extradition treaty between the U.S. and Mexico. Thus, U.S. officers, private individuals, law enforcement officers, or military units could mount an operation to abduct the hacker from the other nation in order to bring him to justice in the U.S. While this approach is a legal option, the international and diplomatic ramifications of an extralegal seizure would be so dramatic and would enter into another realm of military battle.

So, the U.S. could basically kidnap the citizen hacker, or hope that he can be convicted in his host country. Since the U.S. does not have an extradition treaty they can request the hacker be convicted in their host country, nothing will be awarded to the victims, but they will stand trial. However, a conviction will only take place in the host nation's courts if the hacker's virus spread to those nations computers also. (Creekman, 2002) An example of a nation updating computer crime laws is, The People's Republic of China that added computer crimes to the PRC Criminal Code in 1994, making it a crime to delete, alter or disturb the operation of a computer information system so that it does not operate properly. A serious offense is punishable by up to five years in prison and an "exceptionally serious" offense is punishable by no less than five years. In addition, the Chinese government proscribed the deletion of, alteration of, or addition to programs installed in, or processed in transmitted by, a computer system. Unfortunately, the U.S. cannot force the Chinese to prosecute the hacker, nor can it force an extradition of the citizen. Thus, while the U.S. and

China both have relevant laws, but just because the laws exist doesn't mean the laws are used.

Hacker - Vital Target

The U.S. has its hands tied again in its available responses for justice if another nation's citizen hacker were to cripple any of the U.S. critical infrastructures. The affects of such an attack could be catastrophic, and the U.S. is largely paralyzed in its response because the hacker is a private citizen, therefore, making it law enforcement issue. As such, the absence of an extradition treaty significantly limits the retributive responses available to the U.S. government and the victims. (Creekman, 2007)

Regardless of the vital target or the damage that occurs, if a computer attack is attributable to a private citizen with no connection or sponsorship by any government, then the attack must be considered a criminal matter. Like a computer attack on a non-vital U.S. target by an American citizen hacker, an attack on a vital U.S. target would be controlled by the CFAA. (Creekman, 2002) The statute specifically deals with computer related threats to national security. In addition, the statute prohibits the causation of damage throughout the spread of computer viruses or other programs. The same frustrations accompanying the attempted prosecution of a citizen hacker of a non-vital computer system would also, unfortunately accompany any attempt to prosecute a citizen hacking a vital U.S. target. It would be quite difficult to prosecute the hacker because of the absence of an extradition treaty with the other nation. (Creekman, 2002)

Even if there was an extradition treaty between country and the U.S., it is doubtful that an extradition would occur. Most extradition treaties include a political offense exception, which stipulates that a requested party will not grant extradition if the offense is

considered a political offense or connected to a political offense. The nation may view the actions of its citizen hacker as a critique of the American democratic government and therefore, consider it a political offense, absolving the host nation's government of any responsibility to extradite the citizen hacker. (Creekman, 2002)

If an attack caused considerable damage, such as a plan crash resulting from a failure in the air traffic control system, the U.S. could categorize it as a terrorist attack. The international pressure to extradite a terrorist far exceeds any pressure to extradite common criminals. (Creekman, 2002) This increased pressure is due in large part to the perception that the state refusing the extradition request encouraged the terrorist attack. In this case, the host country will want to avoid implication because the complete refusal of a state to cooperate in the suppression of such a hostile act could be considered state sponsorship. This in turn, would invoke the law of conflict management, which authorizes the use of force in self-defense. (Creekman, 2002)

Defensive Counter cyber

The objective of Defensive Counter cyber (DCC) is to protect friendly forces and vital interests from adversary cyber attack. (8TH AFCC, 2007) DCC consists of active and passive cyber defense operations including all defensive measures designed to destroy attacking adversary forces or reduce their effectiveness. Cyber defense includes measures to preserve, protect, recover, and reconstitute friendly cyber capabilities before, during, and after an adversary attack. Currently, cyber defense operations are limited to electronic protection (EP) and network defense (NetD), but should also extend to other terrestrial, airborne, and space based systems that are a part of cyberspace. (8TH AFCC, 2007)

Offensive Counter cyber

Offensive Counter cyber (OCC) operations deny, degrade, disrupt, destroy, or deceive an adversary's cyber capability. (8TH AFCC, 2007) Adversary cyber capabilities include electronics, networks, and other systems that use the EMS. OCC targets include adversary terrestrial, airborne, and space networks; electronic attack (EA) and network attack (NetA) systems; and, command, control, communication, computers, and intelligence (C4I) nodes. As an adversary becomes more dependent on cyberspace, OCC operations have the potential to produce effects that hinder their ability to effectively organize, coordinate, and orchestrate a military campaign. (8TH AFCC, 2007)

III. Methodology

Introduction

The premise of this chapter is to explain how research was conducted for this thesis. For the purpose of this research, a literature review and content analysis was conducted. Since the concept of cyberspace and initiating war within it is a new concept two methods were chosen in which to analysis information on the subject and determine what the core concepts are.

The first method used in this thesis was the literature review. As with all theses the literature review is an important chapter. In this chapter key terms are defined based on your research and identify what are important contributing factors. In this thesis, it was important to highlight these terms because they are key terms that reoccurred in the literature that was found on the subject. Even though the concept of cyberspace has been written about for decades, how it translates to war has been inconceivable since cyberspace is space and not a physical realm. Unlike, physical wars of the past, war fighting in the future will be drastically different. It is important to define terms and determine what common attributes are and how they translate to cyber war.

Content Analysis

A content analysis is a research tool used to review articles, books, and interviews to determine how often certain words or concepts appear. Busch et al., 2005) By using this method for the purpose of this thesis it was possible to determine common themes or areas that need attention as it pertains to cyberspace and war in cyberspace.

For the purpose of this research a conceptual analysis was conducted using Busch et al. and the eight steps for conceptual content analysis. This was the framework, however, the actual analysis used was a combination of the Busch et al. all concept and the Thomas theme, coding and comparison concept analysis. Below are the steps described by Busch et al. with a definition of how the step was used for the purpose of this thesis and how it was applied with the Thomas concept analysis for textual themes. Below is the methodology for this research:

1. Decide the level of analysis.

For the purpose of this research an analysis of certain words was conducted. This research used 33 relevant articles, publications, instructions, and on-line sources to conduct this analysis.

2. Decide how many concepts to code for.

It was recommended by Busch et al. to recognize the key words or phases the researchers are looking for before beginning reading. By combining this concept with the Thomas' themed base approach. (Thomas, 2003) By doing this I was able to evaluate each document and determine the "theme" and was able to categorize the concepts.

3. Decide whether to code for existence or frequency of a concept.

Per Busch et al., the coding frequency means that every time a word or phrase is used, it is counted. Coding for existence, means that once a work or phrase is used it is noted and thee is and it is not counted by how many times it appears in a document. Thomas' contends that each document has a theme and the content can be categorized by theme in order to define the common theme among the research documents. For the

purpose of this research each theme was document and manually tallied based on how many documents included this theme in their reading. The researcher needs to decide on how to distinguish among concepts.

4. Develop rules for coding your texts.

   This research differed in that instead of coding the test it was based on common themes or categories of information. Once all the documents were analyzed for its theme, then that theme or several themes where tallied for that document.

` 6. Decide to do with the irrelevant information.

   For the purpose of this research any irrelevant information was not used.

7. Code the texts.

For this research all tallying was conducted manually. This method has its pros and cons. A pro is that each article is reviewed thoroughly and it allows for the researcher to determine independent themes. A negative is that is done manually, this leaves it open to human error. Another, con was the researcher was the sole coder and therefore, it left the data open to the researchers bias'.

8. Analyze your Results.

Based on the guidelines provided by Busch et al., the researcher is to examine the data and attempt to draw a conclusion about the data. For this analysis it was visually easier to demonstrate the themes and their analysis with frequency tables. Each table gives the frequency the theme occurred in the literature with the relevant information collected and a brief conclusion to explain the date and how it pertains to cyber war.

"It seems one has to accept as inevitable that when something useful for the improvement of man's life has been invented, thoughts will either turn into how to weaponize or destroy it, or, in the case of computer network technology, both."

Louise Doswald-Beck

IV. Analysis and Results

Introduction

The purpose of this chapter is to discuss the findings of information analysis in the literature review and the content analysis. By analyzing the data, the results will answer my thesis question: What constitutes an act of war in cyberspace. The basis for the literature review was to determine how traditional laws of war translate to cyber war and what the attributes of war look like in cyber war. The information revolution based on electronic communications, computers, software and the creation of a world-wide web has had a huge and long running impact on how the USAF fights wars. These technologies have not only changed the way war fighters think of war, but the players have changed, the battlefield and the types of targets as well. With the emergence of the Air Force Cyber Command it has also changed the rules governing military operations and is now recognized by the military as a "real" force. Advances in military technology have out-paced changes in the law of armed conflict and international laws governing how war is conducted. This research focuses on the development of a new type of military and the challenges it poses for the legal regimes that constrain warfare.

Literature Review Analysis

Traditional War vs. Cyber War

In order to compare how traditional war was waged and how it pertains to cyber war, an extensive literature review on cyber war articles was conducted on, Air Force doctrine, LOAC, Geneva Convention, WMD and The Outer Space Treaty. In a traditional sense, war was waged by a formal declaration of war issued by a government indicating that a state of war exists between those nations. Basically, a declaration of war was used to regulate the conduct between military forces during military engagements of the respective countries. The United Nations Charter was created as an attempted to commit the nations involved to using warfare only for defensive purposes. In 1959 however, North Korea invaded South Korea and the United Nations Security Council did not agree with the North Korean action and asked its members to come to the aid of South Korea. Therefore, after World War II Congress limited its use of the power to declare war to issuing "authorization of force." Not using the word "war" is more public relations friendly and by not "declaring war" loosens the constraints for the laws of war. This research revealed that this is where the term "use of force" came from and why it is currently used in times of war.

The international rules governing the "use of force" as stated by the United Nations are Article 2(4) of the United Nations Charter, prohibits any nation form using force against another. The charter allows for only two exceptions to this rule: when force is required in self-defense (Article 15) or when the Security Council authorizes the use of force to protect international peace and security. (Taylor, 2008)

Moving on to today's force, according to the Eighth Air Force Concept of Cyber Warfare Plan, 2007, all military forces and all national agencies maintain capabilities that use particular aspects of cyberspace to accomplish their specific missions. Today's war fighter's first priority is to ensure friendly use of cyberspace as described by the Eighth Air Force Concept of Cyber Warfare Plan. With the use of cyberspace the USAF is able to integrate combat operations across other domains. War fighting in cyberspace is basically a means to countering our adversary's capabilities through our attacks on his systems while defeating any attempts to counter our use of cyberspace. Cyber space is everywhere making it an immense far reaching mission area and going far beyond networks.

Laws Governing War

Laws of Armed Conflict

One the greatest challenges of law, is keeping up with the changes of and advancement in technology. This research has uncovered as many questions as it has answered. Such as, when thinking of law and how it applies to technology militaries don't necessarily think of a physical battlefields and how these laws translate into a cyberspace battlefield. In reference to this research and how LOAC apply, most do seem to loosely convey to cyberspace. Below are the four basic principles of LOAC and an example of how it may translate to cyber war.

1. **Necessity:** Only us the degree of force required in order to defeat the enemy is permitted. In addition, attacks must be limited to military objectives whose nature, purpose or use make an effective contribution to military action and offers a definite military advantage. (Brown, 2006)

Necessity in cyberspace:

Throughout the literature review different authors gave different scenarios of this principle as it applies to information attacks, attacks on most of the enemy's military computer systems are permitted. However, as Brown states in his article if the attacks are aimed at the enemy's stock market or financial systems it seems that would not justify military necessity because this attack would not be seen as a military advantage.

In my research it is also clear that cyber attacks intended to cause widespread environmental damage also are not permitted under the principle of military necessity. One example that Brown used is how information attacks aimed toward the enemy's oil/fuel supplies is seen as a military advantage, but the attacks must be careful to avoid widespread environmental damage such as, the oil well fires set by Iraq in Kuwait at the end of the Gulf War. Another example can be applied to technological attacks by using cyberspace attack a dam and release flood waters. This is permitted if it the action doesn't adversely affect civilian population.

Under LOAC, militaries may not target noncombatants, and may not terrorize them with threats of attack. Although no specific weapons are mentioned in the rules of international law prohibiting direct attacks on noncombatants, it is understood among the armed forces that the rules are meant to govern the physical damage on targets. If traditional and cyber weapons are capable of causing physical damage, then it would make sense that LOAC should make no distinction between them and it should therefore cover cyber war where it applies. Even though one of the benefits of cyber war is the

ability to reduce collateral damage and reconstruction cost. It should fall under the blanket of LOAC because the possibility of physical destruction is very possible.

Another military target that is seen as an advantage is the destruction of bridges, railroads, communications centers, and fuel supplies, and such facilities are justified as lawful targets if they are part of the infrastructure used by the military or are necessary for military mobilization. However, in many cases, these facilities (especially communications centers) support both military and civilian infrastructure. For example, ninety-five percent of communications traffic of the U.S. Defense Information Systems Agency, the lead defense agency operating communications and computer systems serving the entire Department of Defense (DoD), travels on civilian lines available to the public. (Johnson, 1995) The lawfulness of any attack on such dual-use facilities will turn on whether the military advantage gained by attacking the target outweighs the adverse effect on civilians and the civilian population. This principle should apply to attacking infrastructural targets by information attack as well. (DiCenso, 1999)

2. **Distinction:** requires distinguishing military objectives from protected civilian objectives such as places of worship, schools, hospitals and dwellings. (Brown, 2006)

Distinction in cyberspace:

A lawful combatant during military battle has the right to kill enemy forces or drop a bomb or fire on a legitimate military target, but they are not authorized to kill an unarmed civilian. Lawful combatants include the uniformed armed forces of a state (except medical personnel and chaplains) and any forces that satisfy all of the following four

conditions: (1) They are commanded by a person held responsible for his subordinates; (2) they wear a fixed emblem; (3) they carry their arms openly; and (4) they conduct their operations in accordance with LOAC and other customary international laws. (Brown, 2006) Civilians that accompany our armed forces into combat are covered under the Geneva Convention and are to be treated as prisoners of war as the armed forces members themselves. However, nothing in the Geneva Conventions or other sources of international law, grants them the legal right to engage the enemy. Many civilian employees and contract personnel accompanying the armed forces are there supporting the services in areas such as logistics and communications via cyberspace and they are authorized to defend against information attacks, but should be prohibited from engaging in information attacks themselves. That function should lie exclusively with the armed forces, who are lawful combatants. (DiCenso, 1999)

Additionally, LOAC gives protected status to units using distinctive emblem medical units, religious establishments, and specially marked cultural property. Conventional attacks on these sites or areas are prohibited, similarly, information attacks on the computer systems of these protected sites should be treated the same. (Brown, 2006) However, on occasion the protected status of a site may conflict with the right to engage legitimate targets. Traditionally, if a state uses a protected or civilian site in order to shield a legitimate target (i.e. such as putting a command post under a hospital or parking fighter aircraft next to a cultural shrine), then the protected site loses its protection and it may be attacked in order to destroy the military target. (Brown, 2006) This translates to cyber attacks by the military on military computer systems, (i.e.

malicious code) that also house protected sites then the protected systems lose their protection. Just as it is possible to use protected sites as shields against bombs, it is also possible to use protected servers as shields against malicious code. States should be required to separate computer systems with a protected status from those without one. States also should be specifically prohibited from embedding systems that lawful military target in infrastructure that is not protected.

An analogy drawn to computer viruses, all unprotected computer systems are open target to computer viruses, without distinction between combatant and noncombatant systems. An attack on enemy military computer systems using malicious code cannot be considered unlawful per se. However, malicious code such as viruses, worms, Trojan horses, logic bombs, and trap doors, also infect systems used by civilians as well as and they infect computers installed in protected sites such as medical facilities. Malicious code that makes no distinction between lawful and unlawful targets should be prohibited. Military forces already have the obligation to distinguish themselves from civilians, one potential method of making military computer systems similarly identifiable may be to create universally recognized electronic identifiers to correspond with the status of persons and sites under the Geneva Conventions (combatants, medical, chaplain, etc.), much as the red cross and red crescent serve as universal visual identifiers for medical personnel and sites. (Brown, 2006) The use of electronic identifiers and visual identifiers are susceptible to abuse. It's also safe to assume that the malicious code itself can be made smarter, meaning it could be able to identify the likely uses of information systems according to the type of software and hardware they contain or by

the type of networks to which they are connected. For example, U.S. military networks generally us the internet extension ".mil," and hard drives containing medical records or medical laboratory software are likely to be used by protected facilities.

Logic bombs can be compared to landmines in that neither can distinguish between combatants and noncombatants. Landmines have the legitimate purpose of deterring enemy forces from approaching via certain routes. However, abandoned, non-self-neutralizing mines inflict far greater harm to the civilian population. The harm is both physical, due to accidental injuries and deaths to unwitting victims, and economic, in that their presence renders unusable land that could otherwise be used for agriculture or industry. Geneva law prohibits the use of mines and booby traps near concentrations of civilians when no ground combat is taking place, and by requiring their positions be recorded or that they be equipped with self-destruction mechanisms that activate when they are no longer useful for military purposes. Logic bombs are similar in that they lie dormant in a computer system until they are activated--for example, when certain software is run. (Brown, 2006) When activated, logic bombs disable part or all of the system

3**. Proportionality:** requires that military action not because collateral damage which is excessive in light of the expected military advantage. (Brown, 2006)

Proportionality in Cyberspace:

Information warfare as it pertains to proportionality is most evident in the context of responding to malicious code and denial-of-service attack. With today's technology, it

can be difficult if not impossible to trace the source of such an attack if, as most are, the attack is carried out clandestinely. As noted by Ruth Wedgwood:

> If . . . [a country] were the victim of an attack on vital computer systems, the temptation to respond in kind would be considerable. Yet the ultimate source of a computer attack can be acutely difficult to determine--a problem magnified by the deliberate use of "looping" or "weaving"--using another's server to disguise the origination of the attack. An attack is likely to be sent through an unrelated server in order to mask its authorship, and a response in kind may end up damaging or disabling the "looped" server. (Wedgwood, 2002)

In many cases, ghost computers and zombie systems belong to innocent non combatants whose systems or servers have been hi-jacked by malicious code without their knowledge or consent. In this scenario, military forces would have to determine whether defensive measures are adequate to defend against the attack: or if a counter-attack against the attacking server is necessary. If an attack is needed then military leaders would have to decide if the result of an attack against and enemies system is worth the outcome or if it would be detrimental to civilian infrastructure. (Brown, 1999) Leadership will also have to weigh if a counter attack might be possible to deter a future attack. LOAC does not protect noncombatants from being inconvenienced; it protects them only from life-threatening conditions caused by the armed conflict. If innocent parties are harmed in the counter-attack, the responsibility for that harm would lie with the original attacking party who co-opted the innocent systems in the first place.

4. **Chivalry:** requires war to be waged in accordance with widely accepted formalities, such as those defiling lawful “ruses” (e.g. camouflage and mock troop movements) and unlawful treachery (for example, misusing internationally accepted symbols in false surrenders) (Waldrop, 2004)

Chivalry in cyberspace:

1. Prohibition of Perfidy

International law prohibits perfidy, which is defined as an act "inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence." One of the classic examples of this act is pretending to surrender in order to draw the enemy closer, and then firing on them at close range. Yes, this would give the military surrendering the military advantage, but it is deceptive. Some other common examples are pretending to be wounded, misusing protective emblems such as the Red Cross or Red Crescent, and pretending to be a noncombatant or neutral status. By using these kings of activities the enemy then believes that certain forces have a protected status, and should not be attacked, when in fact they have no protected status and are open for attack. (Brown, 1999)

Information technology developments have changed and expanded the methods and effectiveness of committing perfidy in the areas of imaging, spoofing and psychological operations. For example, images of military bases, could be intercepted and morphed to disguise them or make them seem they are located somewhere else. If a military force morphed an image to make it appear that nothing is there would be a legitimate and would not be considered perfidy. However, if an image was morphed to make a military base appear to be a protected site, when in fact it is not, would be perfidy. Sending false communications to mislead the enemy into believing that the sender's forces are in a different location and in a different strength or that they have a

new intent are permissible. But, wrongly making the enemy think a target has a protected status when it doesn't or falsely surrendering is perfidity. (Brown, 1999)

2. Perfidy and Malicious Code

Malicious code is most often propagated by sending e-mail attachments to unsuspecting victims. In order for the malicious code to do its job it must appear inconspicuous, otherwise with all the training military members receive on such e-mails would cause them to delete it and it would not do as it was intended. In a sense, this violates the requirement that combatants be easily identifiable. As long as military forces take reasonable care to distinguish between combatant and noncombatant targets, then information attacks using malicious code would be valid methods of warfare and deserving of regulation.

3. Morphing

The principle of chivalry also does not directly speak to morphing images for propagandistic purposes, using computers to alter reality. An example during the Gulf War is when the Iraqi officials broadcast pictures to the news media of a mosque with its dome missing. However, what actually happened was the Iraqi forces removed the dome in order to make it appear that the U.S. military defaced their mosque. With the advent of new technology morphing is being made easier to fabricate evidence. Images of military forces committing war crimes can be alter to make them look like other forces are actually committing the crime. In the long run these tactics may the war and prolong the duration and cause more casualties and distain. (Brown, 1999)

The Outer Space Treaty

It was not very long ago when for the thoughts of preserving space for peaceful purposes began at the United Nations in the 1950's. In 1957 the U.S. and its allies submitted their proposals for how the treaty should look for reserving space exclusively for "peaceful and scientific purposes," (Ruseck, 2003) but the Soviet Union rejected all proposals based on their preparation to launch the world's first satellite and in order to test its first intercontinental ballistic missile.

The UN resolution of 1884 called on countries to refrain from stationing WMDs in outer space. UN resolution 1962 set legal principles on outer space exploration, stipulating that all countries have the right to explore space. In 1963, these two resolutions became the framework for the Outer Space Treaty. The U.S. and the Soviet Union submitted two separate proposals in 1966. After reviewing both, they came up with a mutually agreed proposal approved on December 19, 1966 and was signed and approved by all parties and entered into force October 10, 1967. (Ruseck, 2003)

Basically the Outer Space Treaty of 1967 bans stationing WMDs in outer space, spells out the legally binding rules of space exploration, and prohibits military activities on celestial bodies. Ninety-seven countries are part of the treaty; North Korea is the only state with real potential for space-launch capabilities that has not signed the treaty. Many countries seem to be concerned with the U.S. missile defense plans and space policy. China has proposed a disarmament agreement in Geneva in the hopes to negotiate a treaty in order to prevent and arms race in outer space. The U.S. insists there is no need for the treaty, because at this time there is not an arms race for outer space.

The basic treaty terms forbid countries from deploying “nuclear weapons or any other kind of weapons of mass destruction” in outer space. In the treaty the definition of WMD is not spelled out, but is to be commonly understood as nuclear, chemical, and biological weapons. One thing the treaty doesn’t address is the launching of ballistic missiles, which could be armed with nuclear warheads through space. The treaty emphasizes that space is to be used for peaceful purposes which could be interpreted as all weapons through space.

The treaty’s key arms control provisions are in Article IV states parties commit not to:

- Place in orbit around the Earth or other celestial bodies any nuclear weapons or objects carrying WMD
- Install WMD on celestial bodies or station WMD in outer space in any other manner
- Establish military bases or installations, test “any type of weapons,” or conduct military exercises on the moon and other celestial bodies

Other treaty provisions underscore that space is no single country’s domain and that all countries have a right to explore it. These provisions state that:

- Space should be accessible to all countries and can be
- Space and celestial bodies are exempt from national claims of ownership
- Countries are to avoid contaminating and harming space or celestial bodies
- Countries exploring space are responsible and liable for damage their activities cause

- Space exploration is to be guided by “principles of cooperation and mutual assistance,” such as obliging astronauts to provide aid to one another if needed (Ruseck, 2003)

International Maritime Satellite (INMARSAT)

International Maritime Satellite (INMARSAT) as stated in AMC Instruction 33-109, International Maritime Satellite Management, is a commercial communication System subject to international law and treaty. It is a radio communication device using a satellite link to interface with terrestrial telephone systems or other mobile terminals. Terminals are commissioned as land, air or sea terminal. Once commissioned, the terminals may be used only in the configuration stated in the commissioning application.

There are 79 countries on the international INMARSAT treaty. One of the provisions of the treaty is that it may only be used for administrative, humanitarian and peacetime applications or under the auspices of the United States. The system may not be used for making war or for example it cannot be used to direct air strikes etc.

Defense Information Systems Agency (DISA) and Defense Information Technology Contracting Organization (DITCO) consider INMARSAT long-haul telecommunications systems per Department of Defense Instruction 46410-14, Base and Long-Haul Telecommunications Equipment and Services.

WMD

As defined by the Department of Defense Weapons of Mass Destruction (WMD) are weapons that are very capable of high destruction and of being used to destroy a large number of people. WMD are generally seen as high damage causing explosives or nuclear, biological, chemical and radiological weapons. (DTIC, 2008)

AF Handbook 10-2502, USAF Weapons of Mass Destruction Threat Planning and Response handbook, states terrorist use of chemical and biological weapons within the United States is a Federal offense under Title 18. U.S. Code (USC) Section 175 for biological weapons possession and Section 229 for chemical or biological weapons use as a WMD. Even when conducted overseas, any property owned, leased or used by any US agency or department, having a chemical or biological weapons attack is a Federal offense, Title 18 USC, Section 229 (4).

AF Handbook 10-2502, USAF Weapons of Mass Destruction Threat Planning and Response handbook, also covers the use of WMD during wartime between nations. It sates that the use of chemical or biological weapons from one nation against another nation is a clear violation of LOAC.

Per DoDD 5100.77, paragraph 5.6, the U.S. Army is the DoD Executive Agent for LOAC violation issues and they are responsible for performing investigations pertaining to chemical and biological weapons use.

An analogy can be made of the effects of computer viruses and from those of biological and chemical weapons. These weapons are clearly effective at neutralizing the combatant forces against whom they are used. Though their targets are very specific

their effects are widespread. Not only are they far reaching but they have the potential to kill far more noncombatants than the combatants such was the case with Iraq's use of chemical weapons against Iranian forces and Kurdish separatists during the Iran-Iraq War. (Brown, 1999) Biological and chemical weapons also inflict unnecessary suffering. Bullets and shrapnel injure more than they kill, they tend to have the same effect without resulting in as many deaths. Biological and chemical weapons kill far more often than they injure, and they have more long-term effects, such as blister agents, far more painful than any long-term injuries caused by conventional weapons. Use of such weapons violates the rule of proportionality, in that it causes collateral damage and seen as an excessive use of force.

In today's world there are not to many transactions that occur that do not involve some type of technology, from transportation, to home computers, electricity, financial institutions and the media to name a few. From living room hackers to terrorist threats attacks are being carried out daily through technology. As defined above WMD are weapons that when used are capable of killing a mass amount of people, it doesn't give a specific number. What is mass destruction? For example, what if a terrorist was able to hack into a power grid on the east coast and take out an entire grid. This would mean no electricity for food, air conditioning, heat, transportation, and medical for millions of people, to name a few. If this were to happen, depending on how long the power was to be turned off then it may kill and injure hundreds and thousands of people. Or what if a hacker was able to take control of a major dam? If they were able to open the dam and release the water, depending on what dam it is, it could kill hundreds of thousands of

people. Both of these examples can easily seen as a WMD and currently it really is not addressed in any LOAC or international laws.

Content Analysis

As outlined in chapter 1, the purpose of this research is to determine what constitutes and act of war in cyberspace. For the purpose of this research an analysis was conducted to determine what laws were involved and how they translate to cyber war as they are written.

The results of the content analysis from the textual data, are presented in frequency table below. The table depicts the theme name, number of relevant articles, number of document the theme appeared and the frequency effect. This methodology allowed for the possibility of identifying more than one theme within a single source.

Table 1. Seven Themes

Theme No.	Theme Name	No. Relevant Articles	Documents containing Theme	Frequency Effect
1	**LOAC**	**33**	**25**	**75.7%**
2	**Hacker Attack**	**33**	**16**	**48.4%**
3	**United Nations Charter**	**33**	**11**	**33.30%**
4	**Attribution**	**33**	**5**	**15.20%**
5	**Outer Space treaty**	**33**	**4**	**12.10%**
6	**Weapons of Mass Destruction**	**33**	**4**	**12.10%**
7	**Offensive/Defensive Measures**	**33**	**2**	**.06%**

Theme 1: Hacker Attack

Theme 1 was the highest calculated Frequency Effect Size of 48.4%, and it was hacker based attacks. The majority of the articles researched saw an immediate need to determine what action should be taken against hackers that are a threat to a nation's security. There are several different scenarios to discuss in this domain. Most of the articles discussed hackers of the citizen nature that were acting on their own behave. For instance if a lone citizen decided to hack into a DoD computer system. If DoD was able to back hack and find the source of the attack they could prosecute the hacker based on the U.S. legal system. However, what would be the consequence if a hacker from another country took over several zombie computers around the world and had all attack our DoD systems on a given day? It would be almost impossible to track the attack back to just one computer system. If DoD would be able to track the attack back to a specific computer to a specific person then, would DoD would have the right to attack them back, and then would their systems be seen as weapons? What if they were military personnel or government workers would this is different if they were civilian? In the Estonia case if they would have been able to track the attack back to a specific person's computer system then per the law they would have had to ask for the governing nation to take action against the person. The U.S. could ask for extradition of the attacker so they could have a trial and punish them, but unless the U.S. has an extradition treaty with the country where it occurred it would not be granted.

The data concludes that the subject of "hacker" based attacks needs to be addressed through international laws. As described in the article by Wingfield, since nation states and non-state actors now have the capacity to use relatively inexpensive and

widely available hardware, software, and expertise to launch "attacks" against their targets the rules that govern them need to be updated. This is a very difficult task since technology is advancing so rapidly and the capabilities of the hackers grow exponentially with the technology, and they share information so rapidly and inexpensively.

Theme 2: LOAC

Theme 2 was the second highest calculated Frequency Effect Size of 48.4%, and it pertains to LOAC. The majority of the articles researched determined current LOAC loosely translate to cyber war. However, many of the authors of the researched articles believed a more serious look needs to be taken at how they pertain to cyber war. To date, the rules and laws of war have primarily been concerned with sovereign borders and physical invasion of those borders by armed belligerents. (DiCenso, 1999) However, in cyberspace there are no borders. Research shows nations are not worried about physical weapons and someone else physically stepping on our soil. Research shows how nations think about information warfare and cyberspace is that they are the new battleground and the terrain of network connections, both owned by military and civilians that interact without regard to lines on a map. The threat comes from the young, the older, techies and not so techies who may be able to disable banking systems, electrical grids, airline traffic control systems, and communications equipment.

Air Force Policy Directive (AFPD) 51-4 (1994), Compliance with the Law of Armed Conflict, par. 2, requires Air Force personnel to comply with the rules "during armed conflict." This directive defines "armed conflict" as a situation where at least one state has begun to use armed force. However, there is no guidance on what constitutes "armed force," obviously it means that one must utilize a physical weapon of some type.

Even with the advent of information warfare and the push to define war in the information age this directive has not been updated to clarify. Better yet, Air Force Instruction (AFI) 51-402, Weapons Review, May 1994, states computer systems would probably not be considered weapon. It states, "Weapons are devices designed to kill, injure, or disable people, or to damage or destroy property. And this instruction states that weapons do not include . . . electronic warfare devices. (AFI 51-402) Even thought computers as not seen as physical weapons, they should definitely be seen as a weapon that could do substantial damage to an enemy's war-fighting capability.

As history shows us, LOAC morphs to encompass the ever changing way war is fought. However, with the emergence of cyberspace and how electronic warfare is conducted, it is not surprising that the LOAC has not kept up with the information age. During World War I, aerial war fare hadn't existed; principles had to be developed from the existing rules. Only after seeing the results of applying land warfare rules to bombing did LOAC change. As the data showed LOAC adapted to new war fighting techniques, as capabilities of other nations to use cyberspace and information warfare to conduct war, LOAC will evolve along with new technology. As the researched demonstrated with the computer attack on Estonia's parliament, computers can cause damage to a nation and its government. In this scenario Estonia claimed that Russia was angry with Estonia's government for moving a Soviet-era war memorial. (Hollis, 2007) They were correct, they were able to trace the attack and arrest the culprit. (Fox News, 2008) Even though the attacker did give a direct hit to Estonia's parliament, nobody was physically hurt, and the computer systems were returned to normal…was this an act of war? Currently, there

is no authority to suggest that a computer is a weapon or that an information operation act is an "act of war." However, if death and destruction would have resulted from this attack, an armed response by the victim nation would probably be warranted.

Based on the research the majority of the authors agree that LOAC needs to be revised. Currently, in armed conflict there exists rules pertaining to POW camps, hospitals, chapels and the Red Cross. However, during cyber war if a virus is sent out via the internet it doesn't denote between combatants and non combatants nor is it able to distinguish between a hospital network and a military network. Another, subject area that needs to be visited when discussing LOAC, is when does cyber war allow for "use of force" in retaliation? Much of the data in this research addressed this issue and all agree that leadership needs to address the subject. A foundation or an outline to follow in order to address attacks with the correct force applicable to the crime needs to be established.

Theme 3: United Nations Charter

Theme 3 the next highest calculated Frequency Effect Size of 33.3%, and it pertains to the United Nations Charter. The many of the articles researched felt the United Nations Charter was in need of revision. As discussed in this research, LOAC authorizes a nation engaged in armed conflict with another nation to attack lawful military targets belonging to the enemy. However, what if a nation is in a peacetime state and has a cyber attack launched on it from another country?

Article 42 of the United Nations Charter allows such action to be taken by air, sea, or land forces that may be necessary to maintain or restore international peace and security. Some examples noted in the research for this article were demonstrations,

blockade, and other operations by air, sea, or land forces of Members of the United Nations. No requirements exist that a "threat to peace" needs to be an attack in the form of an armed attack, a use of force, or any other condition specified in the charter. The Security Council has the authority to decide what constitutes a "threat to peace" and what sort of response is acceptable. (DoD/GC, 1999) Therefore, nothing would prevent the Council from finding that a computer network attack was a "threat to the peace" if it determined that the attack warranted retaliation. However, many of the authors felt the United Nations would not get involved unless a cyber attack were to cause widespread damage to economics or loss of life of a country.

Article 51, requires an "armed attack." Traditionally, this means with physical weapons. However, what if the attacks a cyber attack? (DoD/GC, 1999)

Much of the research discussed the United Nations Charter and determined it was out of touch with today's information warfare and cyber attacks. Unlike traditional war, cyber war is not just physical and it can affect the economy, financial institutions, transportation, during peacetime setting.

Theme 4: Attribution

Theme 4 had a Frequency Effect Size of 15.2%, and it pertains to the attribution of a cyber attack. Once common theme among all the articles detailing cyber attacks was how to attribute where the attack came from and who was conducting it. Just as in the Estonia parliament attack mentioned in this research they were able to track the attack back to the Kremlin. However, they were not able to determine who launched the attack or if the attack was actually launched from within the Kremlin or if that particular

computer was nothing more than a zombie computer. Even though this attack was successful and caused a disruption of parliament, no one was charged with a crime. Another implication would be whether the attacker was a combatant or a noncombatant and if they were acting on their own will or for a nation.

All authors recommend attribution be reviewed and devise a plan for which nations can work together to target, capture and extradite persons responsible for cyber attacks…if it's possible to track them.

Theme 5: Outer space Treaty

Theme 5 had a Frequency Effect Size of 12.1%, and it pertains to The Outer Space Treaty. The Outer Space Treaty indicates that parties agree "not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction. The basic treaty forbids countries from deploying "nuclear weapons" or any other kind of WMD in outer space. In the treaty the definition of WMD is not spelled out, but is to be commonly understood as nuclear, chemical, and biological weapons. One thing the treaty doesn't address is the launching of ballistic missiles, which could be armed with nuclear warheads through space. The treaty emphasizes that space is to be used for peaceful purposes which could be interpreted as all weapons through space. The treaty does not differentiate between cyberspace and outer space. Space law was created to resolve issues around spacecraft or the use of celestial bodies. It will not help resolve any issues the U.S. currently face in negotiating the legal landscape or cyberspace. (DiCenso, 1999)

International Maritime Satellite Management is a commercial communications System subject to international law and treaty. It is a radio communication device using a satellite link to interface with terrestrial telephone systems or other mobile terminals. The terminals are commissioned as land, air or sea terminal. Once commissioned, the terminals may be used only in the configuration stated in the commissioning application. One of the provisions of the treaty is that it may only be used for administrative, humanitarian and peacetime applications or under the auspices of the United States. The system may not be used for making war or for example it cannot be used to direct air strikes etc.

Neither of The Outer Space Treaty nor the INMARSAT addresses their use in cyberspace and cyber war. The treaties state that both are to be used in peace and not to be used as an advantage during wartime. However, what if a cyber attack occurred and the combatants were able to use the satellite to there advantage by tuning it off and flipping it back on or if they just completely shut it down? Like the researchers at the Department of Energy's Idaho National Laboratory generator that they were able to make it self-destruct using computer attacks. (Hollis, 2007). Is it also possible to make a satellite self-destruct with similar attacks?

Again, the consensus is that these treaties are out dated and need to be revisited and re-written to include cyber warfare.

Theme 6: WMD

Theme 6 had a Frequency Effect Size of 12.1%, and it pertains to Weapons of Mass Destruction. The data concluded that WMDs are understood to be nuclear,

chemical and biological. In March 2007, researchers at the Department of Energy's Idaho National Laboratory conducted an experimental cyber attack and managed to make a generator self-destruct. (Hollis, 2007) Computer attacks don't just threaten other computers but the larger infrastructure that controls vital resources. Viruses could become as dangerous as missiles. At the same time, cyber attacks offer militaries the option of disabling an enemy's vital infrastructure temporarily or completely destroying it. If the Department of Energy was able to cause a generator to self-destruct then would an attack on the Eastern sea board power grid be a WMD? If a dam were to be attacked a let out its water and it flood a city is that considered a WMD?

All the research for this paper that pertained to WMD agreed that this is a subject that needs to be revisited. It needs to be understood what is considered a WMD in cyberspace. All authors agree that traditional thinking of this subject needs to disappear and the blinders need to come off and reevaluate the situation.

Theme 7: Offensive/Defensive Measures

Theme 7 had a Frequency Effect Size of .06%, and it pertains to Offensive and Defensive Measures. Based on the research offensive and defensive measures are on the radar. Many of the defensive measures discussed in the data was concerning keeping our adversaries from having a successful attack. Our DoD networks are constantly being probed trying to find a week point for access. Our defensive measures are tested everyday, and the U.S. can never drop our guard.

The offensive measures the research discussed pertained to keeping our adversaries in the dark. The U.S. military has been basically coming up with ways in order to change the data to make it seem like military installations are not there. Both the defensive and the offensive measures will be beneficial for future wars. If the U.S. military is able to counter their attacks and keep them from gaining access to our troop movement, supplies etc., then the U.S. military would have the upper hand. Offensive measures are more useful in war. By fighting offensively, the U.S. stays a step ahead of their opponents by anticipating their next move or by leading them in a different direction. The U.S. military needs to be vigilant in developing these measures and ensure the U.S. stays in keeping with LOAC.

Conclusion

To conclude this chapter, my research gives relevant examples and instances of what could happen in cyberspace, how it can be translated into LOAC and international law as it they are written today. All the services, DoD, Homeland Security and civilian institutions are all starting to address the issue of cyberspace and comprehend the implications on our national defense if the U.S. doesn't address it now. But, the research did not find proposals for new LOAC, international laws and treaties. The research has shown that there are serious implications of a cyber attack and the current laws are not coving what to do if an attack does cause wide spread death and casualties. Some countries do have criminal laws in effect for computer fraud, sabotage and defacement of websites, but there are no laws expanding on attacks between nations and what "use of force" is interpreted as in cyberspace. Not only do laws in the U.S. need to be revisited

in terms of cyber war, but international laws and treaties to be addressed and how cyber war translates to them. If the left hand is not talking to the right, then there are always opportunities for attacks to occur and be successful. Not only is our nation's safety at stake, but the whole world revolves around technology and relies on it everyday. The right attack would be able to cripple not just one nation, but several around the world.

V. Conclusion

Conclusion

The goals of this research effort was to look at laws of armed conflict, international laws and treaties of war and how traditional laws translate to cyberspace in order to answer my thesis question: What constitutes an Act of War in Cyberspace? Based on all the data for this research there is no definitive answer to this question. The data used for my research all gave exceptional examples and scenarios of what could happen and what would be justified as a cyber war. But, nowhere in the data was a generally accepted definition of cyber war and what is considered an "act of war" in cyberspace? The laws have not kept up with technology and the advancement of the individuals launching the attacks. It is obvious that over the decades the way the U.S. communicates and fights has changed drastically. Terms such as IW and cyberspace are not even dialog in any current international laws and treaties. The research showed the way war is fought has changed from bullets and missiles to bits and bytes and therefore the governing laws and treaties pertaining to conventional warfare needs to be changed. It is a fact that our nations critical infrastructure consists of the physical and cyber assets owned and operated by public and private companies that control our critical support structures (i.e. agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous material and postal and shipping to name a few). Thus, cyberspace is the nervous system of our country. Our national security is

dependent upon our leadership's ability to get a grip on cyberspace and what it means to secure it.

The U.S. is at the forefront of the battleground of cyberspace and the initial lead on getting a grip on cyber war. Each service has a "cyber" shop; DoD and Homeland Security each have a division dedicated to cyber war fare. Research shows the U.S. needs to have a national strategy and define how the U.S. will react to cyber attacks. Proportionality needs to be included to state when does a cyber attack constitute a physical attack? For instance if a WMD were to be dropped on the stock market and cause death and destruction and economic turmoil, the U.S. military would have the authority to defend ourselves and react with physical force. Therefore, if a cyber attack was launched and it was able to open up a dam and cause hundreds or thousands of deaths and injuries, causing essentially the same damage...would it also be a WMD? Would the U.S. military have the authority to react with physical force when the initial attack itself was not physical, but cyber? The U.S. and our allies, need to be able to answer when is it ok to act based on "use of force" and "self defense" in cyberspace.

These laws need to incorporate contractors, privately owned networks and civilian institutions into the equation. Almost all of our critical infrastructures is supported by or owned by privately owned companies. Contractors are an important part of our daily mission and they are critical to our national security, our military needs them to aid in the fight and ensure the security of our national assets.

Once the U.S has a national overview and sight picture, then the U.S. needs to encourage and enlist the help of its allies in a re-write of current international laws of war with the U.N. Council. Just as LOAC, the Geneva Convention, Hague all give a template for how militaries conduct themselves in physical war, militaries need to have the same template that conveys to cyber war. Therefore, based on my research there is no definitive answer as to what constitutes an act of war in cyberspace. The data did not define or pin point an action or a trigger that would translate to all situations. The concept of cyber war is so new and there are so many moving parts and players it makes it difficult to imagine all scenarios and how they should play out in war. The data in this research concluded that cyber war is real and on the minds of many leaders. It is being taken more seriously and steps are being taken to get a grasp on what needs to be the next step. With the standup of the AFCYBER Command, the USAF will see changes in how cyber war is viewed in the near future.

Recommendations

Throughout this research more questions were asked than were answered. Based on this research and the lack of a definition for cyber war and no concrete rules of engagement in cyberspace, it is recommended that the leadership of all nations in the U.N. need to address all international laws governing cyber war. To start, a universal definition of cyber war needs to be established. In addition, all laws conveying to traditional war (i.e. LOAC, WMD, U.N. Charter, attribution, etc.) need to be revised and/or re-written to incorporate cyber war and cyberspace. The ramifications if

cyberspace is not address in these international laws are endless. If these laws are not re-written it is giving hackers free rein to launch attacks against whomever and whenever they like. Today, the DoD computers and computers of other national governments are being probed daily, sometimes thousands of times a day. One reason for this is the U.S. is the best military in the world, thus causing other countries to find new avenues in order to compete with the U.S. military. In cyberspace countries are able to compete for the fraction of the cost since no military or expensive machinery is needed. In cyberspace the battleground is the same for every player and currently there are no international laws pertaining to cyberspace. However, more nations are incorporating computer laws into their criminal laws and as in the Estonia case they are able to prosecute criminally if they are able to prove who launched an attack.

Cyberspace is such a vast entity and new concept it is impossible to include everything into one thesis. The following paragraphs provide some topic areas for future research in areas related to the identification of cyber war and what constitutes and act of war in cyberspace.

Define cyber war. This definition is key to incorporating cyber war into the revision of international laws. Without a universal definition these laws will not be able to be revised or re-written.

When does cyber war engage in physical war? Many of the articles for this research indicated that there needs to be a determining factor for when cyber war turns

into physical war. Currently, there are no clear definitions of when this should occur or what would justify a physical attack.

What are the attributions of cyber war? What actions of cyber attack should be reacted upon? If the U.S. was attacked by a denial of service attack and the source can not be determine, then when is a counter denial of service attack feasible?

Weapons of Mass Destruction. When is a cyber attack considered a weapon of mass destruction? What should the criteria be for defining a cyber attack as an act of war and how does the U.S. update current international laws and treaties to reflect that?

Jurisdiction and Information Warfare Investigation. The information requirements analysis method developed in this research could be used to construct new laws used to back hack attacks to what criminal laws may apply to the attacker. If it is possible to identify the host nation and define who may cross international boards for intelligence collection the U.S. may have a better chance at actually capturing the attacker.

Cyber Battle Plan. Due to the newness and lack of international laws pertaining to cyber war a type of cyber battle plan would be helpful. The U.S. needs some type of plan that gives different scenarios and what legally the U.S. can do based on the type of attack received.

Offensive and Defensive Cyber Operations. Offensive Counter cyber (OCC) operations deny, degrade, disrupt, destroy, or deceive an adversary's cyber capability.

OCC targets include adversary terrestrial, airborne, and space networks; electronic attack (EA) and network attack (NetA) systems; and, command, control, communication, computers, and intelligence (C4I) nodes. As an adversary becomes more dependent on cyberspace, OCC operations have the potential to produce effects that hinder their ability to effectively organize, coordinate, and orchestrate a military campaign.

Defensive Counter cyber (DCC) is to protect friendly forces and vital interests from adversary cyber attack. DCC consists of active and passive cyber defense operations including all defensive measures designed to destroy attacking adversary forces or reduce their effectiveness. Cyber defense includes measures to preserve, protect, recover, and reconstitute friendly cyber capabilities before, during, and after an adversary attack.

Offensive and Defensive cyber attacks will need to be researched further in order to understand the scope of cyber war and assist in the writing of cyber laws.

Summary

This research presents a method for identifying what constitutes and act of war in cyberspace. Chapter I presented and overview of the research and background information to cyber war.

Chapter II provided background information that enables the reader to understand key research concepts related to the complexity of identifying cyber war and what

actually constitutes an act of war. In this chapter LOAC, the Geneva Convention, WMD and The Outer Space Treaty were covered.

Chapter III presented the methodology used in this research. For the purpose of this research a literature review was conducted and content analysis of cyber war and how it pertains to the way militaries traditionally declared war, how cyberspace fits into the constraint of war today, Weapons of Mass Destruction, The Outer Space Treaty and INMARSAT. In order to do this a literature review of cyberspace in military doctrine, Air Force cyberspace doctrine, LOAC, and international laws, WMD, The Outer Space Treaty and the INMARSAT treaty was conducted. Then a content analysis of the data was conducted by a themed approach by coding and comparing the textual information and displaying it in frequency tables.

Chapter IV applies the methodology from Chapter III and gave an analysis of the literature review and a content analysis. The content analysis was conducted by a themed approach by coding and comparing the textual information and displaying the common themes in frequency tables.

Chapter V provides conclusions from this research and suggests potential areas for future research related to the identification of what constitutes an act of war in cyberspace.

Appendix A: Glossary of Terms and Abbreviations

8TH CC – Air Force Core Concept Plan

AFCYBER - Air Force Cyberspace Command

AFI – Air Force Instruction

AFPD – Air Force Policy Directive

AMC – Air Mobility Command

C4I - Computers and Intelligence

DCC – Defensive Counter Cyber

DISA - Defense Information Systems Agency

DITCO - Defense Information Technology Contracting Organization

DoD – Department of Defense

EA - Electronic Attack

INMARSAT - International Maritime Satellite

LOAC – Law of Armed Conflict

NetA - network attack

OCC - Offensive Counter Cyber

U.N. – United Nations

WMD – Weapon of Mass Destruction

Bibliography

Air Mobility Command (1998). International Maritime Satellite Management. AMCI 33-109. Wright-Patterson AFB: HQ AMC/SCYC.

*Aldrich, Richard W. (1996), "The International Legal Implications of Information Warfare." USAF Institute for National Security Studies, USAFA CO.

*Arquilla, John, (1999), "Can Information Warfare Ever be Just? *Ethics and Information Technology*, 1,3, pp 203-210 .

Barker, Garry (2004) "Alert but not Alarmed: The Mac Man." *The Age (Melbourne, Australia),* 2 September 2004, Green Guide. Livewire:7.

*Bayefsky, Anne (2007), "Geneva Conventions", *The Wall Street Journal.* 21 June 2007, pg. A16.

*Bennet, John (2007), "USAF: Cyber War Needs New Laws, Not More Money." http://defenseNews.com

*Brooks, Peter (2007), "A View From the States" http://www.righthinker.com

*Brown, Davis (2006), "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", *Havard International Law Journal*, Vol. 47, Number 1, Winter 2006:179.

*Buchan, Glenn (1996), "Information War and the Air Force: Wave of the Future? Current Fad?," *Issue Paper Rand*. March 1996.

Busch, E., et al. (2005), "Content Analysis," Writing @CSU. Retrieved 3 March 2008. http://writing.colostate.edu/guides/research/content/index.cfm

Bush, G. W. (2003), "The National Strategy to Secure Cyberspace," Washington D.C. The White House.

*Condron, S. (2007), "Getting it Right: Protecting American Critical Infrastructure in Cyberspace," Harvard Journal of Law & Technology, Spring, Vol 20, No 2, pp 404-422.

*Creekman, Daniel (2002), "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China." *American University of International Law Review*, Vol 17, pp 641.

Department of Homeland Security (2003) "National Strategy for Homeland Security. "National Strategy to Secure Cyberspace." February 2003.

Department of the Air Force (1994), "*Compliance with the Law of Armed Conflict,* AFPD 51-4. Washington: HQ USAF.

Department of the Air Force (2001), "*USAF Weapons of Mass Destruction Threat Planning and Response Handbook,"* AFH 10-2502. Washington: HQ USAF.

Department of the Air Force (1994), " Weapons Review," AFI 51-402. Washington: HQ USAF.

Department of Defense (1998), "*Law of War Program,"* DoDD 5700.77.

Department of Defense, General council (1999) "*An Assessment of International Legal Issues in Information Operations"*

*DiCenso, David (1999), "Information Warfare Cyber law: The Legal Issues of Information Warfare." A*irpower Journal*, Summer 1999

*Eighth Air Force Concept of Cyber Warfare. 1 June 2007

Estonia Charges Solo Hacker for Crippling Cyberattacks. January 2008. http://forxnews.com/printer_friendly_story/0,3566,325547,00.html

Friedman, Herb (2007). Deception and Disinformation. 30 November 2007. http://www.psywarrior.com/DeceptionH.html

Geneva Conventions (2008), Geneva, Switzerland, Diplomatic Conference for the Establishment of International Conventions for the Protection of Victims of War, 1949.

Geneva Conventions (2008). World Almanac & Book of Facts (serial online). 2008:858-858. Available from: Academic Search Premier, Ipswich, MA.

*Glennon, Michael J. (2002), "The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter," *Harvard Journal of Law & Public Policy*. Vol 25. Spring 2002.

*Graham, Bradley (2003), "Bush Orders guidelines for Cyber Warfare," *The Washington Post., 7* February 2003.

Hague Convention, 1954 Hague Conv. § 8(l)(a)-(b), 249 U.N@.T.S. at 246.

*Hampton, Stephens (2007), "War in the Third Domain," *Air Force Magazine*. April 2007

*Hoffman, Michael (2003), "The Legal States and Responsibility of Private Internet Users Under the Law of Armed Conflict: A Primer for the Military on the Shape of Law to Come," *Washington University Global Studies Law Review*. Vol 2

*Hollis, Duncan (2007), "Rules of Cyberwar?," *Los Angelos Times*, 8 October 2007, Sec. A:15

Johnson, Philip (1995), "The International Legal Implications of Information Warfare." AFP 110-34. Headquarters USAF/JAI. October 1995.

*Jormakka, Jorma (2008), "Use of Networks in Asymmetric Warfare Why We do not See More of Cyber Warfare," *National Defense College, Department of Military Technology*.

*Kaar, Jason (2007), "The Emergence of International Terrorism and Technological Changes: Have These Changes Made the Law of Armed Conflict Obsolete?," *Military Medicine*, Vol 172, December Supplement 2007

*Kimball, Daryl (2003), "The Outer Space Treaty at a Glance," *Arms Control Association Fact Sheet*. September 2003.

Kuschner, Karl (2007), "Legal and Practical Constraints on Information Warfare," *Airpower Journal, 3 Dec 2007.*

*Leyden, John (2008), "Government War Gamers Hack Servers to Stay Ahead," *The Register*. 1 February 2008

*Leyden, John (2008), "Isreal Suspected of Hacking Syrian Air Defences," *The Register*. 1 February 2008

Louise, Doswald-Beck (2002), "*Some Thoughts on Computer Network Attack and the International Law of Armed Conflict"*, 76 Int'l L. Stud. 163, 163

*Lubrano, Alfred (2006), "Search for Terrorists Find a traitor," *Jewish World Review*. 5 May 2006

Maney, Kevin (2003), "If U.S. Launches Cyberattack, it Could Change Nature of War," *USA Today*, 12 February 2003, sec. Money:3B.

*Mazzola, Cory (2006), "Legal Implications of Warfare in the Information Age," *Norwich University Journal of Information Assurance*. Vol 2 No 1.

Melnick, Jim (2007), "The Cyberwar Against the United States," *The Boston Globe*, 19 August 2007, Sec. OP-ED:E9.

*Miller, Robert (1997), "International Law How it Affects Rules of Engagement and Responses In Information Warfare," The Research Department, Air Command and Staff College. March 1997.

*Parks, Raymond (2001), "Principles of Cyber Warfare," *IEEE Workshop on Information Assurance and Security*. June 2001.

*Paone, Chuck (2007), "Air Force Leaders Discuss Need To Control Cyberspace." Address to the Fifth Annual Net-Centric Operations Conference. New Castle, N.H. 26 October 2007.

Powers, Ron (2006). Laws of Armed Conflict: The Rules of War. 30 November 2007 . http://usmilitary.about.com/cs/wars/a/loac.htm

*Randle, Jim (1999), "Millennium: Futurewar in cyberspace," Pentagon Background Paper, 15 December 1999.

*Rasch, Mark (2004), "Why the Dogs of Cyberwar Stay Leashed," *The Register*. 24 March 2004

Rowe, Greg (2006), "Applying Principles of War," Winter 2006 http://www.maxwell.af.mil/info-ops/iosphere/iosphere_win06_rowe.pdf

Schmitt, Michael (1999), "Computer Network Attack and the use of force in international law: Thoughts on a Normative Framework." June 1999

*Shulman, Mark (1999), "Legal Constraints of Information Warfare." Center for Strategy and Technology Air War College, Air UniversityMaxwell Air Force Base.

*Sharp, Walter Gary, Sr. (1999), "Redefining National Security in Today's World of Information Technology and Emergent Threats," *Duke Journal of Comparative &* International Law. Vol 9. 1999.

Sun Tzu (1968), The Art of War, Thomas Cleary (Boston, Mass; Shambhala Publications, distributed by Random House, 1968).

Taylor, Rachel (2008). International Law, the United Nations and the War in Iraq E:\ThesisResearch\A Worldpress_org special report - International Law, the United Nations, and the War in Iraq - Worldpress_org.mht

Waldrop, E. (2002), "Intergration of Military and civilian Space Assets: Legal and National Security Implications," Air Force Law Review, Spring, Vol 55, pp 157-231.

Wedgewood, Ruth (2003), "Proportionality, cyberwar, and the Law of War." 76 Int'l L. Stud. pp. 219, 222.

*Wilson, Clay (2007), "Information Operations, Electronics Warfare, and Cyberwar: Capabilities and Related Policy Issues." *CRS Report for Congress*. 5 Jun 2007.

Wingfield, Thomas C. (2006), "*When is a Cyber Attack an "Armed Attack*?" *The Potomac Institutute for Policy Studies*. 1 February 2006.

*Wingfield, Thomas C. (2004) "An Introduction to Legal Aspects of Operations in Cyberspace." *Naval Postgraduate School*.

Wynne, M. W., & Moseley, T.M. (2205). *SECAF/CSAF letter to airmen: Mission Statement*

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
24-03-2008	Master's Thesis	March 2007 – March 2008

4. TITLE AND SUBTITLE

What Constitutes an Act of War in cyberspace?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Kelli S. Kinley

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/08-M12

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

INTENTIONALLY LEFT BLANK

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT In December 2005 a new mission statement was released by the Air Force Leadership, "to deliver sovereign options for the defense of the United States of America and its global interests...to fly and fight in Air, Space and Cyberspace." (Wynne & Mosley, 2005) With the stand up of the AFCYBER command and the use of cyberspace to carry out our daily mission the U.S. needs to have a clear understanding of what war in cyberspace looks like and what the laws are governing war in cyberspace. This research and it's resulting data analysis is intended to provide a better understanding of what the current laws of war are and how they translate to cyber war and the complexities that exist, along with recommendation on future revisions of the laws.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. Dennis Strouble
U	**U**	**U**	**UU**	69	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 3366 (dennis.strouble@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18