COMPUTER NETWORK ATTACK AND THE LAWS OF ARMED CONFLICT: SEARCHING FOR MORAL BEACONS IN TWENTY-FIRST-CENTURY CYBERWARFARE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

MATTHEW E. HABER, MAJ, USAF
B.A., University of Pittsburgh, Pittsburgh, Pennsylvania, 1987
M.S., Troy State University (European Region),
Troy, Alabama, 1994

Fort Leavenworth, Kansas
2002

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Matthew E. Haber

Thesis Title: Computer Network Attack and the Laws of Armed Conflict: Searching for Moral Beacons in Twenty-First-Century Cyberwarfare

Approved by:

_____, Thesis Committee Chair
Major Matthew T. Phillips, M.B.A.

_____, Member
Major Joanne P. T. Eldridge, J.D.

_____, Member, Consulting Faculty
Colonel E. Wayne Powell, J.D.

Accepted this 31st day of May 2002 by:

_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the forgoing statement.)

ABSTRACT

COMPUTER NETWORK ATTACK AND THE LAWS OF ARMED CONFLICT; SEARCHING FOR MORAL BEACONS IN TWENTY-FIRST-CENTURY CYBERWARFARE, By MAJ Matthew E. Haber, 117 pages.

Computer network attack ushered in change for the profession of arms. Militaries achieve effects using computers, previously attained only through physical destruction. Computer network attack's problem is it operates outside the observable domain the laws of armed conflict describe, yet its effects are what the laws address. Thus, the primary research question is: Does a legal framework of analysis exist for computer network attack? The secondary question became: If a framework exists, is it applied consistently throughout the Department of Defense? A search of literature and interviews with information operators and their associated lawyers revealed a framework by Thomas Wingfield. The framework analyzes the level of force but does not address the four basic principles for warfare; military necessity, humanity, proportionality, and discrimination. Also, the framework is not applied throughout the Department of Defense. The Joint Task Force Computer Network Operations' creation is the first step in building a hierarchical structure for consistent application of law to computer network attack. Research recommends such a structure expand Wingfield's framework for computer network attack to be a viable weapon for Twenty-First-Century Warfare.

ACKNOWLEDGMENTS

This thesis is far from complete without a few words of thanks to those who contributed significantly. Their efforts ensured the thesis' finest features and the author claims responsibility for any inaccuracies. The thesis committee is first on the list. They worked tirelessly offering advice and counseling. They were also a great source of encouragement for keeping the effort on track and on time. I also offer thanks to each of the individuals who took time out of their busy schedules and answered the interview questions. Their candid responses made this thesis more complete and hopefully relevant. The United States Command and General Staff College's Graduate Degree Programs staff was first-rate. Particular thanks goes to Helen, who fielded more than her fair share of questions, sacrificed hundreds of hours to proofreading students' work, and somehow managed to smile through it all. Finally, a special thanks goes to my family. Most of my reading and typing was done from home and their patience and encouragement was a key ingredient for success.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

CHAPTER 1

WHEN WARFARE OUTPACES THE LAW

A New Weapon in the Arsenal

Computer Network Attack

The explosion of information technology ushered in a new era of change for the profession of arms. Armed forces, like the rest of society, began relying on information technology to manage their daily affairs. Personal computers, e-mail, networks, cellular phones, satellite communications, video teleconferencing, etc. became standard lexicon for modern military forces. But there is a less visible, more potent side of information technology, the capability to affect one's enemy. Effects previously attainable only through physical destruction are now accomplished remotely with the silent hands of information technology. Force is no longer unique to the physical world. Force now comes in the form of computer network attack through complex networks.

The effects of computer network attack are potentially no less devastating than those wrought by more physical means. For example, consider the use of military force to cut off electrical power to an enemy's military installation. Traditional use of force might include the precision bombing of the power plant, the cutting of power lines, or the seizure and shut down of the power facility. All of these options required a physical destruction in enemy territory to produce the desired effect. Today, a computer operator remaining in his home territory might use computer network attack to alter lines of code in the power plant's automated control software triggering a shut down sequence and causing the plant to cease operations. The approach is different but the result is the same.

New applications of military force generate legal analysis. The profession of arms, like other professions, is subject to legal constraints. Past changes in approach to warfare were mostly in the physical domain and therefore easily observable from initiation to conclusion. Each new approach was analyzed, parallels were drawn to previous approaches, legal constraints were applied as appropriate, and where legal constraints were deemed insufficient changes or additions were made. Computer network attack is different. It operates almost exclusively outside the physical domain and is not easily observable from initiation to conclusion. Remembering that effects of computer network attack are potentially similar to that of more physical approaches, this thesis seeks to answer the questions: "Is there a framework for applying law when considering the employment of computer network attack?" If so, "is the framework applied consistently throughout the Department of Defense?"

A View to Twenty-First-Century Warfare

National, armed service, and civilian documents and literature highlight the importance of information technology. The United States' National Security Strategy for a Global Age states, "We also are committed to maintaining information superiority" (The White House 2000, 20). It goes on to state, "We must keep pace with rapidly evolving information technology so that we can cultivate and harvest the promise of the knowledge that comes from this information superiority, sharing that knowledge among U.S. forces and coalition partners while exploiting the shortfalls in our adversaries' information capabilities" (The White House 2000, 20). Air Force Basic Doctrine outlines counterinformation as 1 of 17 air and space power functions. Counterinformation includes cyber attack (Headquarters Air Force Doctrine Center 1997, 53). The United

States Army's newly released Field Manual 3-0, *Operations*, dedicates an entire chapter to information superiority including a section on offensive information operations (IO). That section states, "The desired effects of offensive IO are to destroy, degrade, disrupt, deny, deceive, exploit, and influence enemy functions" (Department of the Army 2001, 11-2). Finally, Edward Waltz, a recognized expert and frequent lecturer in the field of information warfare (Waltz 1998, 383), in his book, *Information Warfare: Principles and Operations*, says, "In the twenty-first century, information may become the very essence and manifestation of competition, conflict and warfare" (Waltz 1998, 2). The United States, its armed forces, and scholars seem to agree the future of armed conflict will feature information warfare. They agree in another area as well. Legal challenges exist where information warfare is concerned.

Military Force and the Law

Militaries choose force options based on a number of influences. Cost, effectiveness, availability, and public opinion are considerations that vary in the amount of influence each brings to bear at any given time. Laws, however, are a more consistent guide to choosing military methods of employed force. Specifically the laws of armed conflict, *jus in bello*, guide the way nations fight for the benefit of combatants and noncombatants (Roberts and Guelff 1982, 1). The Hague Convention of 1907, the Geneva Conventions of 1949, and the additional Geneva Protocols of 1977 are three of twenty nine treaties that outline the conduct of warfare and in some manner impact the potential use of computer network attack (Wingfield 2000, 14). Former Air Force lawyer Major David DiCenso noted, "Whether war is waged on the muddy fields of Verdun by shell-shocked infantry troops or a high-tech cyberspace battlefield, the rules and general

principles of the [laws of armed conflict] remain applicable" (DiCenso 1999, 93). Four basic principles of the laws of armed conflict drive the analysis of computer network attack; military necessity, humanity or unnecessary suffering, proportionality, and discrimination or distinction (United States Army Command and General Staff College, Student Text 27-1 2001, 5-7 - 5-8). The principle of military necessity is defined as, "any action not forbidden by international law which is indispensable for securing the complete submission of the enemy as soon as possible" (Department of the Army 1956, 3-4). Use of the words "any action" avoids the more specific label "armed conflict" and thus the principle of necessity accommodates the consideration of computer network attack. Humanity and unnecessary suffering are principles whose nomenclature and meaning stand on their own, though one should note that these principles apply for any lawful use of arms in a manner that would otherwise cause unnecessary suffering. The third principle, proportionality, directs, "The anticipated loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained" (Department of the Army 1956, 19). Again, there is no specific mention of "armed conflict" in this statement lending additional credence that these principles are more concerned with outcomes than means of attack. Finally, discrimination and distinction require distinguishing between combatants and non-combatants and between military objectives and protected property or places (Protocol Additional to the Geneva Conventions 1977, Article 48). These four principles are the underpinnings of the Geneva Convention's articles and other bodies of international law guiding armed conflict.

The United Nations Charter and international conventions also influence the use of force. Article 42 of the United Nations Charter permits use of force to restore peace, after all other avenues are exhausted, to include demonstrations, blockades, and "other operations." (Charter of the United Nations 1945, Article 42). Both of these articles make no requirement that the force be "armed." The United Nations Charter and other bodies of international law do assume combat is inherently a physical affair between sovereign nation states. The preamble of the United Nations Charter refers to, "our respective governments," (Charter of the United Nations 1945, preamble) and other bodies of international law use the terms "civilized nations" and "states parties" (Roberts and Guelff 1982, 30). These nation states acknowledge the laws of armed conflict are dynamic and ". . . evolve along with new technology and the warfighting capabilities of [those] nations" (DiCenso 1999, 94).

Scholarly work relating information warfare to bodies of law is sparse. A few authors have used the laws of armed conflict and international treaties to analyze portions of information warfare. Their analysis often leads to conclusions such as, "However, for now, we have only the existing law and must apply it as best makes sense, working to fill the law's gaps as they are identified" (Aldrich 1996, 26). Needed is a body of work that provides in-depth analysis and recommends a means for filling those gaps. Such a text was authored by Thomas Wingfield of the Aegis Research Corporation and provides the first evidence that a framework for applying law to information operations exists. The text is examined further in chapter 2 and forms the basis for analysis in chapter 4. Examining the breadth of information warfare and conducting legal analysis are beyond the scope of this thesis. Instead, this work narrowly focuses on computer network attack,

a small slice of information warfare, and answers several questions: Are the laws of armed conflict applied to computer network attack? How are they applied and by whom? Are they applied consistently? What challenges exist in applying law to computer network attack? What are the best means for resolving those challenges? The specific answers for computer network attack have value however, this research should hopefully provide a more valuable process for analyzing other areas of information warfare.

Computer Network Attack, Armed Conflict or Other Means?

Defining Armed Conflict

A central issue to this thesis is whether computer network attack is a form of armed force. The merit of this issue stems from the title given the rules overtly written to address military combat: the laws of *armed* conflict. Most works relating computer network attack to law call into question the term "armed." The issue, though addressed, is not examined in full detail to either validate or repudiate computer network attack as a form of armed force. Most of these works assume that computer network attack is not armed force but do not suggest the evidence for such a conclusion. "In the absence of conclusive legal authority indicating, say, that particular information warfare attacks are 'armed attacks,' 'aggression,' or 'force,' the United States can act with some confidence that its acts will not be held to be so," is a typical conclusion (Greenberg, Goodman, and Soo Hoo 1998, 94). But what legally binding documents, treaties, decisions, and charters were examined and what did they say on the subject even if not conclusive? What was the definition of "conclusive" in the author's mind? Was it the absence of the direct mention of information warfare attack or was it the precise definition of armed attack?

These questions form the thesis' foundation. Examining existing laws and definitions is necessary before any analysis or conclusions may be formed.

Defining a New Force With Old Terms

The laws of armed conflict, while not specifically addressing computer network attack, offer guidance on the use of force. Section two of the 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land addresses hostilities. Article 23 specifically prohibits belligerents, "to employ arms, projectiles, or material calculated to cause unnecessary suffering" (Convention (IV) 1907, Article 23). The same article also prevents attackers from, "[destroying] or [seizing] the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war" (Convention (IV) 1907, Article 23). Lastly, article 25 states, "The attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended is prohibited" (Convention (IV) 1907, Article 25). These articles use language transferable to any type of force. The words "material" and "by whatever means" open a door for inclusion of future weapons. Also, articles addressing effects such as "destruction" and "seizure" make no prerequisite on the type of force employed. Examining each article and its applicability to computer network attack is a tedious process. Seventy years after the 1907 convention, a new protocol explicitly required such an examination.

The first 1977 Protocol Additional to the Geneva Conventions made specific reference for consideration of new weapons. Part III, Section 1, Methods and Means of Warfare, Article 36--New Weapons states, "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under obligation to determine whether its employment would, in some or all

circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party" (Protocol Additional to the Geneva Conventions 1977, Part III, Section 1, Article 36). This statement obligates a nation, at the very least, to consider the laws of armed conflict before employing computer network attack. That consideration should focus on both the means of force and perhaps more importantly on the effects.

Effects Based Warfare

One potential means of linking the transparent properties of electronic warfare to laws designed for more physical armed force is by studying effects. Brigadier General David A. Deptula in his paper, *Effects Based Operations: Change in the Nature of Warfare*, summarizes the concept of effects based warfare when he says, "An alternative concept of warfare is based on control--the idea that an enemy organization's ability to operate as desired is ultimately more important than the destruction of the forces it relies on for defense" (Deptula 2001, 11). Advocates for this type of thinking argue that levels of destruction, probabilities of destruction, and physical annihilation are far less important than the outcome of warfare in terms of an enemy's capabilities. Thomas Wingfield concurs with this line of thought when he says, "The realization that [computer network attack] can be used to attack the basic infrastructure of our civilization is only slowly dawning. In this case, the frightening aspect is not the means, but the end" (Wingfield 2000, 182). The key to this concept is understanding the linkages in an enemy's systems, forces, leaders, and social fabric. This understanding enables friendly forces to pinpoint weaknesses for precise engagement. These engagements are not always the result of physical force. Deptula points out that, "Non-lethal weapons and

information warfare should enhance the ability of our forces to conduct operations to directly achieve desired effects" (Deptula 2001, 23). If this is the case, than perhaps the laws of armed conflict can be interpreted based on effects. This thesis examines the four underlying principles of the laws of armed conflict and seeks language that addresses effects or outcomes as a result of combat. Laws that address effects may translate more easily to computer network attack.

Definitions

The following definitions are provided as points of clarification and for reference. These terms are used consistently throughout the thesis with respect to the definitions provided below.

Collateral damage: Unintended and undesirable civilian personnel injuries or material damage adjacent to a target produced by the effects of friendly weapons (Department of the Army 1997, 1-30).

Combatant: One taking part in armed combat. Engaging in combat (Morris 1973, 265).

Computer network attack: Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device

to destroy a computer's electronics and causing the same result is EA (Chairman, Joint Chiefs of Staff 1994, 98).

Information operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems (Chairman, Joint Chiefs of Staff 1994, 223).

Information Superiority: That degree of dominance in the information domain which permits the conduct of operations without effective opposition (Chairman, Joint Chiefs of Staff 1994, 223).

Information Warfare: Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW (Chairman, Joint Chiefs of Staff 1994, 224).

Law of armed conflict/law of war: That part of international law that regulates the conduct of armed hostilities (Chairman, Joint Chiefs of Staff 1994, 264).

Non-combatant: A person connected with the armed forces whose duties are other than fighting, such as a chaplain. A civilian in wartime (Morris 1973, 892).

Offensive information operations: The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack (Chairman, Joint Chiefs of Staff 1994, 331).

Principle of discrimination and distinction: This principle requires that combatants be distinguished from non-combatants, and that military objectives be distinguished from protected property or places (Protocol Additional to the Geneva Conventions 1977, Articles 48 and 51).

Principle of humanity or unnecessary suffering: Combatants may not use arms that are per se calculated to cause unnecessary suffering and may not use otherwise lawful arms in a manner that causes unnecessary suffering (Convention (IV) 1907, Article 23e).

Principle of military necessity: A commander may take any action not forbidden by international law which is indispensable for securing the complete submission of the enemy as soon as possible (Department of the Army 1956, 3-4).

Principle of proportionality: The anticipated loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained (Department of the Army 1956, 19).

Thesis Structure

Chapter Design, Annexes, and Source Documentation

This thesis is constructed with five basic sections; an introduction, a literature review, an overview of methodology used, the analysis, and a conclusion. Each section constitutes one chapter. Annexes follow the final chapter and provide information on the interviews conducted during the course of research. Annex A is a list of interview questions. Annex B is a list of the people interviewed. Finally, Annex C contains the typed notes from the interviews. Sources are documented throughout the thesis using the parenthetical method. A complete list of cited works follows the annexes and a

bibliography of all works considered is included to aid other researchers in identifying potential sources.

Limitations and Delimitations

The primary limiting factor of this thesis is the narrowing of the topic to computer network attack. Though the broader terms of information warfare and information operations are addressed, the discussion and analysis are reserved for the specific topic of computer network attack. The aim of the thesis is to determine whether a framework for applying law to computer network attack exists. If so, then is that framework consistently applied throughout the Department of Defense? The thesis will not attempt to establish the adequacy of any existing framework but rather will only prove the validity of any framework as it applies to computer network attack. Hopefully, such a framework could be adapted to other forms of information operations not addressed in this thesis.

If a framework does not exist, then this thesis will recommend approaches for constructing and employing a legal framework for computer network attack. This body of research will not attempt construction of a legal framework but rather examines processes and organizational structures that might facilitate its creation. The hope here is that recommended processes and organizational structures identified in the concluding chapter will not only apply to computer network attack but also to other disciplines of information operations.

Two other significant limitations also define the scope of research and analysis. First, this thesis only examines computer network attack as used by the militaries of sovereign nation states. Further, only the United States military is considered to facilitate

the ability to research the topic thoroughly. The second major limit is the assumption that the United States military has crossed the threshold from events leading to conflict into combat activities. The United Nations Charter in article 2 (4) defines this threshold as force used, “against the territorial integrity or political independence of any state” (Charter of the United Nations 1945, Article 2 (4)). This limitation also narrows the scope of research and allows for better comparison of computer network attack to other means of force employed during war.

The cut-off date for seeking sources was established as 31 December 2001. The date was chosen to facilitate the actual construction of the thesis and its submission to the faculty of the Army's Command and General Staff College. Sources found after this date were either brought to the author's attention by thesis committee members, interview subjects, or through daily media.

CHAPTER 2

LITERATURE REVIEW

Source Types and Topics

Source Types

Three types of sources were used to construct this thesis. No one source type should be construed as more significant than another, however, each brings its own relevance to the study. First is the use of scholarly texts. These books cover their subject matters more thoroughly and their construction is often more professional than other written materials. The drawback to published books, especially when relating to information technology, is their timeliness. Even the most recently published texts are based on research normally greater than a year old. Study on information technology is thus forced to use published texts as sources that serve as a foundation, or comparison, for more current findings.

The latest relevant research was incorporated into this thesis by examining academic articles, monographs, and news releases. Less comprehensive than a full text, these sources remain a solid means of examining critical thought with the added advantage of currency. One caution when using recently released articles is their credibility. As each source is detailed below, special attention is given to the credibility of the written piece by examining the author, the author's sponsor (if any) and the raw data presented. The format of these sources is split between hardcopy and electronic formats. Where possible, the thesis uses a combination of books and articles by the same author for greater continuity and more fully developed concepts.

The final type of source used is primary documents. Primary sources were found in the areas of laws, conventions, treaties, doctrines, and official government documents. There are fewer primary sources than any other type but their importance to the research is greater than all other sources combined. These sources serve as the foundation for building a research framework. They offer the basis for analysis and conclusions. The reader may disagree with the conclusions of this thesis, however, primary sources should go unquestioned as to their accuracy and credibility.

Topics

Four topic areas categorize the research: the nature of future conflict, computer network attack, law, and computer network attack and the law. The first of these, the nature of future conflict, provides relevancy to the topic. The nature of future conflict will determine the role of computer network attack. This category attempts to answer the questions, “So what?” and “Why should I care?” The nature of future conflict also provides a contextual setting for the research. Sources in this category give the reader a better understanding of the motivation behind the study.

The next two categories define the thesis' core topics. The category “computer network attack” aids in understanding the complexities of the subject and the potential consequences of its employment. “Law” includes the various legal documents, conventions and treaties that guide or constrain the use of computer network attack. These two categories form the basis of understanding before constructing the analysis phase of the thesis.

The final category is computer network attack and the law. Sources in this category relate the core topics and serve as a means for examining the analyses of others.

This thesis identifies previous analyses and gaps where no analyses exist. This category goes directly to answering the primary questions of whether a legal framework exists that guides the employment of computer network attack and if such a framework is applied consistently by the United States military.

The Sources

The Nature of Future Warfare

Two primary sources offer a vision and direction for the conduct of future conflicts. *A National Security Strategy for a Global Age* and *Joint Vision 2020* highlight the importance of harnessing information technology to achieve information superiority. Two sections of the United States national security strategy in particular, "Responding to Threats and Crises" and "Preparing for an Uncertain Future" address information technology and its importance to the security of the United States (The White House 2000, 19 and 29). *Joint Vision 2020* goes further by stating a specific vision for information technology and its employment by United States armed forces. It defines information superiority as, "transitory in nature and must be created and sustained by the joint force through the conduct of information operations" (Chairman, Joint Chiefs of Staff 2000, 8). It also acknowledges the fact that, "While the goal of achieving information superiority will not change, the nature, scope, and 'rules' of the quest are changing radically" (Chairman, Joint Chiefs of Staff 2000, 8). This statement acknowledges, at the very highest level of the United States military, that the rules governing information superiority are subject to inquiry. The document therefore indicates the future direction for United States' armed forces and provides a reason for asking the thesis' primary question.

Several other sources expound on future conflict and contain a broad analysis based on the aforementioned primary sources. First among these is the recently published Quadrennial Defense Review (QDR). The QDR focuses on capabilities to counter new and emerging threats. "Initiatives in counterterrorism, missile defense, advanced weapons, and information operations are examples of programs that are underway to reduce future challenges risk" (Secretary of Defense 2001, 71). The document sheds light on the importance of these programs by stating, "The Department will treat information operations, intelligence, and space assets not simply as enablers of current U.S. forces but rather as core capabilities of future forces." (Secretary of Defense 2001, 46). A related text to the Quadrennial Defense Review is, *QDR 2001: Strategy Driven Choices for America's Security*, a collection of essays by the National Defense University QDR 2001 Working Group. The text states, "Information warfare will become increasingly important," and goes on to specifically identify computer network attack as a growing means of information warfare (Tangredi 2001, 42). This book also offers two unique perspectives for other research beyond the scope of this thesis. The essays were intended to jump start the QDR process and so serve as a basis for comparing the final product to some of the original input to the review. More importantly, the essays were constructed in April of 2001, before the tragic events of September 11th. This fact may help discern any change in the Department of Defense's views on information attack.

The final group of sources presents potential scenarios for information operations and more specifically, computer network attack. Among these are *War and Anti-War*, *Grand Strategy for Information Age National Security*, and *Future War: An Assessment*

of Aerospace Campaigns in 2010. These sources serve the purpose of understanding the context of how computer network attack may occur in the near future and potential consequences. Futurists Alvin and Heidi Toffler's *War and Anti-War* introduces the concept of "third wave war" where technology is the driving enabler of military capabilities (Toffler 1993, 10-11). They expand on this concept in the chapter entitled, "War Without Blood?" in which they consider means of attack using non-lethal weapons (Toffler 1993, 132). The specifics of these means are vague, however, the consequences or effects are as real for electronic weapons as they are for their more physical counterparts.

The second text, *Grand Strategy for Information Age National Security,* contains a useful scenario entitled, "The Day After. . . In Cyberspace," that outlines a variety of futuristic capabilities (Kennedy, Lawlor, and Nelson 1997, 69-7). Among these capabilities are computer network attack as a means to shut down telephone switches and power facilities, modify oil flow through pipelines and traffic controls for rail transportation, and corrupt data in financial and military data systems (Kennedy, Lawlor, and Nelson 1997, 69-71). Three military officers wrote this monograph while attending Harvard University's Kennedy School of Government as National Security Fellows. While the focus is on defense, it serves as a valuable source to understand the types of computer network attacks information technology promises for the future.

Finally, *Future War: An Assessment of Aerospace Campaigns in 2010,* details potential attack scenarios for the United States Air Force that leverage computer network attack (Barnett 1996, 115-150). The author, Colonel Jeffery Barnett, was the Military Assistant to the Director, Net Assessment, Office of the Secretary of Defense. He

specifically outlines how computer network attack is used to effect national communications and transportation grids and the military's air defense and command and control capabilities (Barnett 1996, 132 and 150). These works substantiate computer network attack's prominent role in the future capabilities of the United States military and show likely roles for its use.

Missing pieces of literature on this subject are sources arguing against the likelihood of information operations and computer network attack in future warfare. Though it seems unlikely that any academic text would dismiss this type of warfare completely, the possibility does exist. Perhaps more likely, are works addressing scenarios where computer network attack would be inappropriate. These works might offer reasons for not using electronic force including legal constraints. Future works addressing these concerns would be helpful in further defining a legal framework for the application of computer network attack.

Computer Network Attack

The next category of sources explains thoroughly the concept of computer network attack. Though there are no primary sources that exclusively claim origin for the concept, military doctrine documents define the term. Among these are Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 3-13, *Joint Doctrine for Information Operations,* Air Force Doctrine Document 2-5, *Information Operations,* Field Manual 3-0, *Operations,* and Field Manual 101-5-1, *Operational Terms and Graphics*. These bodies of doctrine provide the military view toward information operations and computer network attack. Joint Publication 3-13 provides the most comprehensive overview of information operations from the military

perspective. It outlines the, ". . . operational guidance for information operations in the joint context throughout the range of military operations" (Chairman, Joint Chiefs of Staff 1998, I). More specifically it addresses offensive information operations and the organizational requirements for such capabilities. Air Force Doctrine Document 2-5 gives a service unique perspective on offensive information warfare. The document shows potential effects for such warfare at the strategic, operational and tactical levels (Headquarters Air Force Doctrine Center 1998, 28-29). The document fails however to clearly show the organizational structure required at the individual service-level (Headquarters Air Force Doctrine Center 1998, 34-35), a concept that chapter 4 explores further. Equally important to the thesis are the definitions and perspectives of civilian subject matter experts.

Two texts serve as sources for understanding information warfare and its subsets, information operations and computer network attack. Martin C. Libicki's *What is Information Warfare* and Edward *Waltz's Information Warfare: Principles and Operations* are comprehensive works on the subject. Libicki's book is a good introduction to information warfare. At the time of its writing in 1995 however, he acknowledged, "The global information infrastructure has yet to evolve to the point where any of these forms of combat is possible. . . " (Libicki 1995, 75). Its contents define and categorize the different aspects of warfare's electronic means. Despite the infancy of computer network attack, Libicki foresees "semantic attack" capabilities where a system appears to function normally but with corrupted data (Libicki 1995, 77). The Waltz text is a much more detailed and technical source.

Edward Waltz has worked for over thirty years as an engineer specializing in signal and data processing applications for the defense industry (Waltz 1998, 383). *Information Warfare: Principles and Operations* offers models for computer network attack including the one shown in figure 1. This model shows computer network attack fitting into the means labeled "information (electronic) attack" (Waltz 1998, 6). The model also shows the ability of computer network attack to affect an enemy's observations and orientation of the attack. Finally, Waltz notes in his text that computer network attack against, "computers or links controlling physical processes, such as power plants, pipelines, and machinery, can cause destruction in the physical domain" (Waltz 1998, 7). The major advantage of this work is its deliberate and objective approach to the subject.

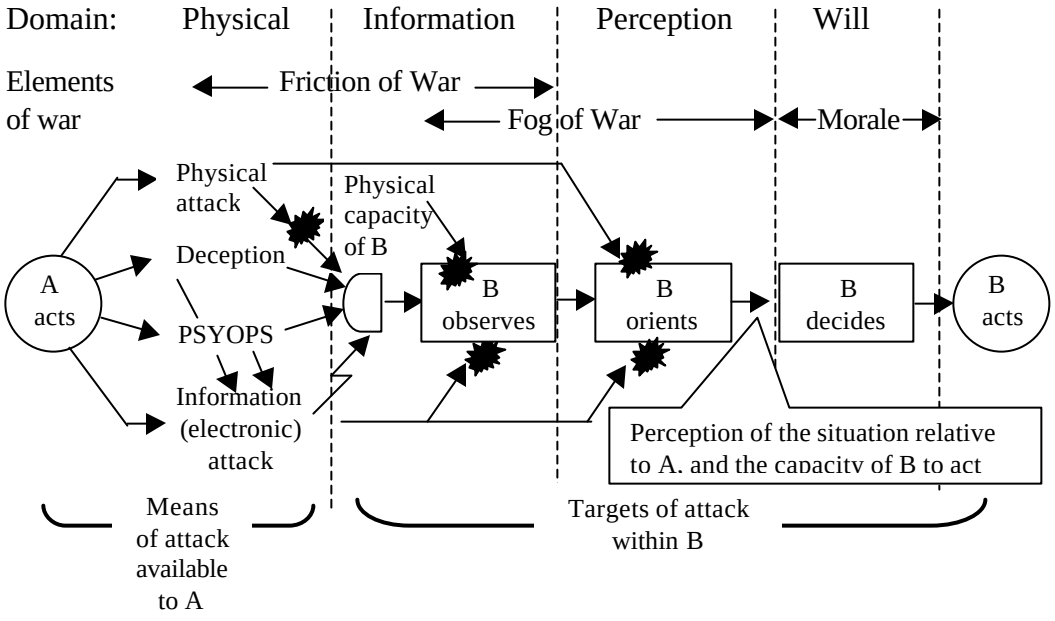

Figure 1. A basic model of the information process in a conflict between attacker A and defender B. (Waltz 1998, 6)

Works that analyze information warfare and its component computer network attack include *Cyberwar*, a collection of essays by various authors and John Arquilla and David Ronfeldt's *The Advent of Netwar*. The first book's advantages are its variety of perspectives from a number of subject matter experts and its coverage of various aspects of information warfare. In one article entitled, "Information Warfare: The Future," John L. Peterson, the founder of the Arlington Institute for studying the changing nature of security, relates computer network attack to the thoughts of Sun Tzu. He says, "warfare is about achieving behavior change, and the highest art is to accomplish that change without a single shot being fired" (Peterson 1996, 224). One might assume "no shot being fired" would result in fewer adverse effects to an enemy however, Winn Schwartau, known as the "civilian architect of information warfare" (Campen, Dearth, and Gooden 1996, 295), shows how computer network attack can lead to collateral damage (Schwartau 1996, 246-247). Schwartau's article, "Ethical Conundra of Information Warfare," looks at the second and third order effects of computer network attack. He argues that a nation cut off electronically from the outside world would suffer economic consequences over time and therefore people could potentially die from the lack of healthcare or food (Schwartau 1996, 247). *Cyberwar* gives breadth to understanding computer network attack.

The Advent of Netwar is a report prepared for the Office of the Secretary of Defense by the RAND Corporation's National Defense Research Institute. This report is useful for understanding how computer network attack leverages the advantages of network infrastructure to conduct non-linear, non-sequential operations. These qualities

allow the attacker to act at any given time, in any given place to gain a set of advantages over his enemy (Arquilla and Ronfeldt 1996, 100).

The remaining sources in this category round-out varying perspectives on the subject. Paul Strassman's The Politics of Information Management recognizes the importance of clear policy and organizational structure for the success of computer information attack. Finally, *Information Warfare and Security* by Dorothy E. Denning is true to its title. An entire third of the book is dedicated to offensive information warfare. She describes computer network attack as a means of fabricating or distorting information similar to Martin Libiki's "semantec attack." She also discusses denial of service attacks that limit or shut off an enemy's ability to access certain systems (Denning 1999, 104-108). The text is useful in the sense that it provides a link between the concepts of computer network attack and nation's security.

Law

Sources in this category provide an understanding of the laws, treaties, charters, and conventions that may influence the conduct of warfare. Primary sources do exist in this area and include the Geneva Conventions and Protocols and the United Nations Charter. Each of these documents serves as the basis for interpretation and analysis. The Geneva Conventions and Protocols are often referred to as the laws of armed conflict and have guided the conduct of warfare for more than a century. The protocols serve as a unique source because they were driven by technical and social changes. Their study offers insight into potential expansion of existing laws of armed conflict. The United Nations Charter specifically states reasons a nation may engage in warfare including self-defense and when all other means of influence have failed (Charter of the United Nations

1945, Article 42). Also, article 2 (4), as explained earlier in chapter 1, provides the measurement for when a nation is considered to be at war. What is missing from published material is the process or framework that allows changes to the laws of armed conflict. It would be useful to know the forces and mechanics behind these changes in order to draw any relevant parallels to information warfare and specifically to computer network attack.

The second types of primary sources in this category are domestic laws. Though not addressed by the scope of this thesis, these laws specifically address the means of information warfare. Unfortunately, many experts agree the law is just now catching up to new technologies while others argue the attempt is distanced by technology's increasingly rapid advance. Existing laws are often based on older technologies but they serve as potential sources for analogies to newer computer means and capabilities. Most recently, the Council of Europe proposed a new convention on cybercrime. This is one of the first conventions to address the issue of computer network attack directly albeit from the perspective of law enforcement vice conflict. The treatment of the subject, however, still offers new perspectives on the legalities in the international community.

Beyond the primary sources are works that explain and analyze their content. Books on the various principles of the laws of armed conflict such as Geoffrey Best's *Humanity in Warfare* help define law in depth. The detail of their analysis aids in applying these age-old principles to modern computer-age warfare. Other texts analyze the applicability of laws to the conduct of war. The Laws of War, a collection of essays that examine the application of the Geneva Conventions and Protocols over history, offer breadth to the topic. Again, what's missing are published materials on the background of

how they were actually changed. What appears in the current texts are the more obvious effects that drove change. What is not covered is the dynamic that drove international players to agree to consider the changes.

Computer Network Attack and the Law

The final category of sources is those relating law to the discipline of computer network attack. This area is also sparse in the number of published materials though their frequency is increasing. The advantage in this category is the currency of the available material. Most were published in the last two years. Only one comprehensive scholarly work exists in this area, Thomas Wingfield's The Law of Information Conflict: National Security Law in Cyberspace. Wingfield works for the Aegis Research Corporation and writes and lectures frequently on the subject of information warfare and more specifically, computer network attack. He provides a basic framework of analysis based on the law of armed conflict's principles of military necessity, unnecessary suffering, proportionality and discrimination. His work forms the foundation for analysis in chapter 4.

Lieutenant Steven M. Barney of the United States Navy took a different approach to cyberspace and the law. “Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace,” by Lieutenant Barney is a logically argued analogy for prescribing law to computer network attack. His essay identifies potentially similar phenomena between ships at sea and information in cyberspace such as the law of transit and innocent passage. Barney's work falls short however, in recommending processes and structures for incorporating his ideas.

Nearly all other sources that relate computer network attack to the law do so in general terms. Among these are *Information Warfare and International Law, The International Legal Implications of Information Warfare,* and *IW Cyberlaw: The Legal Issues of Information Warfare*. Each looks at broad aspects of information warfare and what laws may or may not apply. Their approach is descriptive rather than prescriptive. All three works serve a useful purpose as a launching point to identify primary sources of law relating to computer network attack. These materials also begin to develop useful analogies and scratch the surface of some of the key issues when applying law to computer network attack.

CHAPTER 3

METHODOLOGY

Approaching the Topic

Personal Interests and Experiences

Personal interests and experiences influence the selection of a specific thesis topic. Those influences are an important consideration for understanding the motivation and credibility of the author. Members of the profession of arms conduct warfare based on centuries-old concepts of codified fairness and civility (Best 1980, 23). These norms for fighting do not impede capabilities or the lethality those capabilities bring to bear on the enemy. Each time new capabilities are introduced to warfare, the United States and other nations have addressed these changes with new interpretations of previous laws for armed conflict or created new ones. Such was the case for airpower's rise at the beginning of the Twentieth Century (Biddle 1994, 140-141). As information technology is introduced to the battlefield it would seem logical that those same laws and rules of engagement would again come under review.

A large influence is the communications and command and control experience gained through fifteen years of service on behalf of the United States Air Force. In those fifteen years an average office has gone from one or two computers per squadron to nearly one computer per worker. Alert status boards for nuclear strike aircraft have changed from grease pencils and man-in-the-loop information relays to high-tech state of the art walls of electronic information. This evolution in military affairs is the result of technology becoming second nature in our work places and on the battlefield. The pace of this evolution carries a price.

The Air Force Communications Agency (AFCA) is home to the Air Force's only law office that deals exclusively with information technology legal issues. It seems the demand for legal guidance concerning the employment of information technology is increasing exponentially as reflected in the doubling of staff for AFCA's legal office (Laedlein interview, 5 March 2002). These professionals fight to keep pace with rapid changes in capabilities. As Colonel Charles Laedlein, USAF (Retired) and Director of AFCA's Information Technology Law Office says, “IT law is a growth industry” (Laedlein interview, 5 March 2002). One area where law appears to be losing, or perhaps ignoring the fight, is in the area of information operations.

As the profession of arms becomes fully integrated into the digital world we are reminded daily of its perils. Each time a government computer is turned on, banners greet the operator with various warnings and caveats for use. Every military professional is trained to create complex passwords and identify potential viruses. Information assurance through information protection is key to continuous operations. But what are we protecting ourselves from? And if an adversary poses a threat to our systems, are we not ourselves capable of executing these same capabilities? If so, the United States possesses a new weapon in its arsenal.

Scratching the Surface

Knowledge that physical destruction might now be possible by electronic means drove the search for literature relating the laws of armed conflict to computer network attack. As mentioned in the literature review, works relating law to the powers of information technology are scarce. Some sources go to the extreme of suggesting the laws of armed conflict do not apply to cyberwarfare. This thought seems incredible.

Have there ever been such claims at the advent of other new weapon systems? Did protestors of airpower claim that because aviation brought a new dimension to the battlefield and used a previously unused medium that it should be exempt from the laws of war? No, they did not. In fact, they incorporated laws prohibiting the aerial delivery of "projectiles and explosives" from balloons and sought to ban the use of aircraft by militaries (Roberts and Guelff 1982, 121). The banning of chemical and bacterial weapons is another example of nations restraining themselves in the conduct of warfare (Roberts and Guelff 1982, 137-138). Precedents thus exist for applying law to new means of warfare.

This thesis presumes the laws of armed conflict apply to computer network attack. This may at first seem biased. Upon closer examination there are only two answers as to whether law applies to information operations; either yes it does, or no it does not. Though the author is inclined to assume that information operations are subject to law, the justness of this belief is inconsequential to this thesis. If at some point in time information operations are declared exempt from the laws of armed conflict, than the results of this thesis become invalid. This thesis is not an emotional crusade to champion the cause of law where information operations are concerned. This thesis simply establishes a logical argument for applying law to computer network attack. It also determines whether any process or framework exists for applying the law to cyberwarfare.

A framework for applying law to computer network attack should address *jus in bello*. The concept of *jus in bello* is defined as the laws that are applicable once war begins. These laws regulate the conduct of war and include the Hague Regulations and

Geneva Conventions and Protocols (Nabulsi 2002, 1). Writers, scholars, and governments refer to these laws as "customary" or in some cases "international humanitarian law" (Nabulsi 2002, 1). In contrast, *jus ad bello* includes the laws that nations apply before hostilities. (Nabulsi 2002, 1) These laws help determine the justness of an impending conflict. This thesis limits the examination of computer network attack to its use once warfare begins.

A framework of analysis should also address a second, and closely related, characteristic. Having established the requirement for addressing *jus in bello*, the framework should examine the general principles of the laws of war: military necessity, unnecessary suffering, proportionality, and discrimination. These principles form the foundation for customary law where conflict is concerned. A framework addressing these principles, as criteria, will aid planners of computer network attack in determining the acceptability and suitability of the planned action. Without such a framework, operators may find the use of computer network unfeasible.

Choosing a Methodology

Challenges of Qualitative Research

Qualitative research is primarily an exercise of critical thinking and analysis. What distinguishes one type of qualitative research from the next are the tools and methods used to develop the analysis. The construction of a perfect methodology in the approach to a thesis is of little value if the chosen tools are not available to the researcher. The challenge is selecting enough appropriate and available tools that will provide a meaningful and scholarly work. The construction of this thesis was accomplished while attending the Army's Command and General Staff College in Ft. Leavenworth, Kansas.

The school schedule precluded the possibility of extensive travel as a means of gathering data. The first criteria for method selection was the necessity to conduct research from one location. The second criteria was the deadline for completion by May of 2002.

Discourse Analysis

The limits of location and time led to the selection of discourse analysis as the primary means of conducting the research. Discourse analysis is the study of others' works and looking critically at the motivations and biases behind those works (University of Texas 2001, 1). Fort Leavenworth's Combined Arms Research Library (CARL) offers a wide variety of scholarly works on information operations and the laws of armed conflict. This thesis capitalizes on the research of others and uses discourse analysis to avoid the pitfalls of bias. The goal of this thesis is to examine as many points of view as possible to arrive at facts, reasonable assumptions, and objective conclusions. Discourse Analysis thus, "will not provide absolute answers to a specific problem, but enable us to understand the conditions behind a specific problem" (University of Texas 2001, 1). The second task of this research was to make sense of the data.

The logical question outline in figure 2 focused research and data collection. The basic logic flow: 1) defines computer network attack, 2) examines the criteria used in the definition, 3) determines whether those criteria give cause for analysis using the laws of armed conflict, 4) searches for a framework of analysis using the general principles of the laws of armed conflict, 5) determines whether such a framework is applied and 6) suggests reasons for either success or failure in applying a given framework.

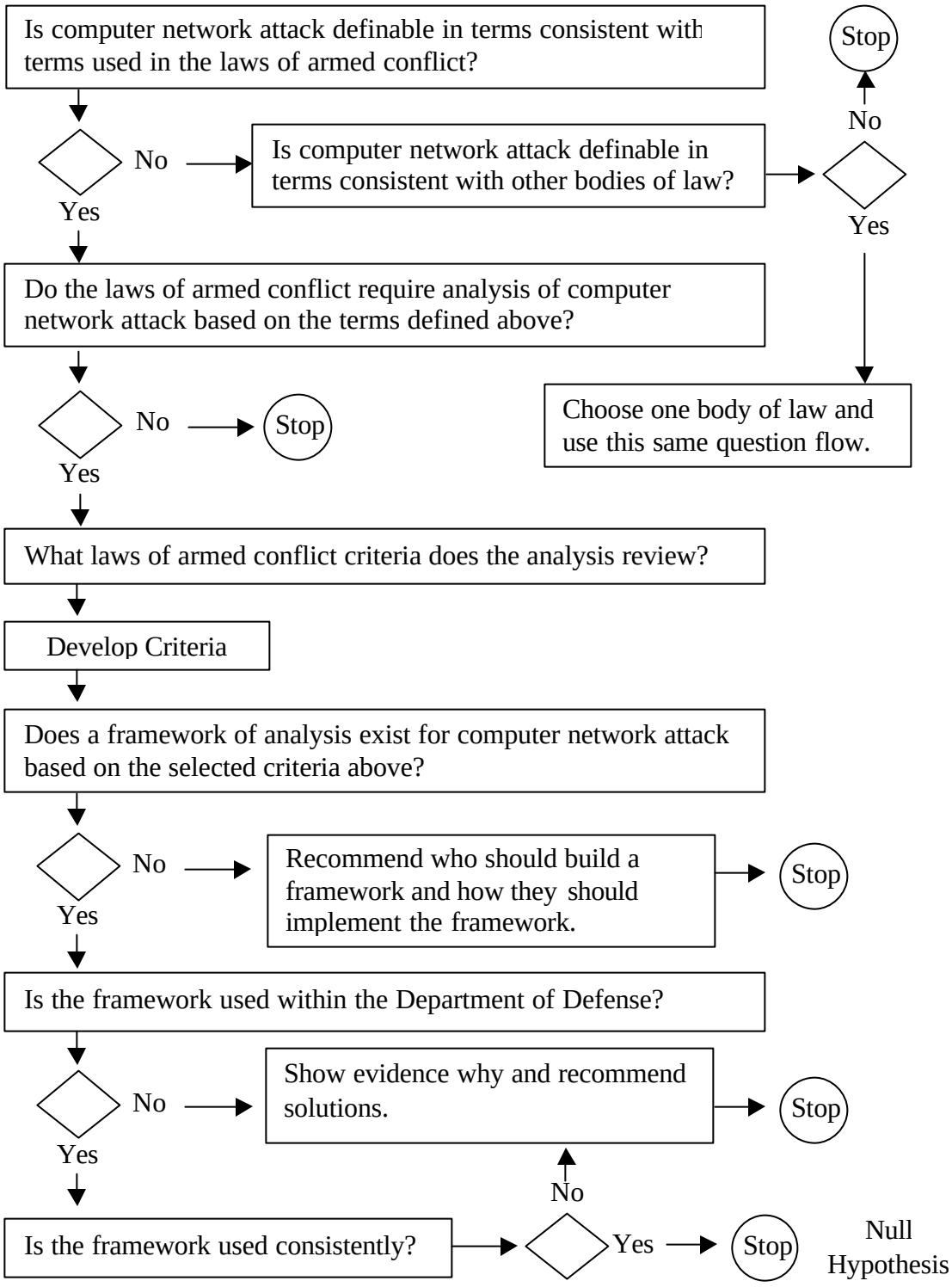

Figure 2. Thesis Question Flow

Original Research

One final tool used in the construction of this thesis is a series of interviews. The interviews targeted two types of individuals, computer network attack operators and the lawyers who provide counsel to those same operators. Because the target audience was small the survey combined closed and open-ended questions. The interviews were conducted by telephone and open-ended questions were used to fully develop answers. Interview questions and responses determined the need for a framework of law to guide computer network attack, whether such a framework existed, and if used was it consistently applied. The interviews also aided in contacting scholars, lawyers, and operators in the field of information operations. The end result was a meaningful product that drove useful conclusions and recommendations listed in the final chapter. A copy of the interview questions, a list of interviewees, and the interview notes are found in appendixes A, B, and C respectively. The interview notes do not reflect the names of the interviewees to provide each person academic freedom and non-attribution in their responses.

Plan of Attack

The Objective

Before building any plan it is important to understand the objective. The objective of this thesis is to follow the logical question outline to answer the primary questions: Is there a framework for applying law to computer network attack? And if so, is the framework applied consistently? There are two critical components to the study. The first is understanding what computer network attack is and how it occurs. The second is identifying and understanding laws that impact the use of computer network

attack. A legal framework of analysis should provide a link between the two. Such a framework is not intended as a panacea solution for applying law to computer network attack but rather a guide for sound judgement and decision making.

Selecting Sources

The primary consideration when selecting sources is credibility. Establishing credibility required examining the background of authors and in many cases the background of the institutions sponsoring or publishing the research. The research focused on authors who were subject matter experts and institutions that focused on particular areas of study. A secondary consideration was balance. If a specific avenue of research tended to lean in one direction, it was important to look for credible sources countering those views. Almost always it was easier to find sources confirming presupposed beliefs and it took more effort to find sources opposed to those beliefs.

Once the sources were selected, the research focused on collecting and organizing facts, assumptions, and opinions. The reasoning for this technique was to support the logical question flow of figure 2. Facts provided the strongest evidence for any particular question and mainly came from primary sources. Next, came assumptions divided into two categories. The first consisted of assumptions deliberately made to narrow the scope of research. The decision to consider computer network attack's use beyond the United Nations threshold for war is an example of a deliberate assumption. The second category was assumptions weighted by the evidence of the research. Finally interview responses were used to analyze the data to support conclusions shown through discourse analysis.

Thesis Mechanics

The completion of the thesis was greatly aided by the expert advice and constant oversight of the thesis committee. Each chapter was drafted separately, reviewed and redrafted until satisfactorily completed. The structure and timelines of this thesis were in accordance with the requirements of *Student Text 20-10: Master of Military Art and Science (MMAS) Research and Thesis*, 2001, provided by the United States Army Command and General Staff College, Fort Leavenworth, Kansas.

Expectations

This thesis should highlight a useful tool for applying law to computer network attack or suggest a means for producing such a tool. On a larger scale, it is hoped that the methodology for deriving that tool and some of its components might also be useful in developing a framework for applying law to other forms of information operations.

CHAPTER 4

A LEGAL FRAMEWORK FOR CYBERWARRIORS?

Analysis Roadmap

Computer network attack, as a new means of military force, is subject to scrutiny under the laws of armed conflict. This analysis answers the primary questions, "Is there a framework for applying the laws of armed conflict to computer network attack?" and if so, "Is the framework applied by information operators charged with executing computer network attack? Analysis begins with demonstrating the need for a framework. Two areas address this issue; first are the requirements levied by the laws of armed conflict and second are the responsibilities of command. The next phase of analysis shows whether a framework exists and the acceptability of such a framework. In other words, "Is there an existing framework that covers the four general principles of the laws of armed conflict introduced in chapters 1 and 2?" The third and final portion of analysis shows if and how the laws of armed conflict are applied to computer network attack.

The methodology for this analysis is covered in-depth in chapter 3, however, a brief review is provided here. Two chief methods of research served as the foundation for analysis and conclusions. The first method, discourse analysis, was a thorough review of existing documents and professional works. The second was a series of interviews conducted with information operators charged with computer network attack and the legal counselors assigned to those same operators. Annex A contains the list of base questions used to conduct the interviews. Annex B lists the interviewees and their contact info. Finally, Annex C consists of the transcribed interview notes. The first

method establishes a foundation for analysis while the second drives original thought on the current state and future requirements of applying law to computer network attack.

New Weapons and the Laws of Armed Conflict

Cyberattack: Weapon, Armed Force, or Other Means?

> So, those sophisticated at using forces neutralize an adversary's military power, but not through battles; occupy an adversary's cities, but not through siege; and destroy an adversary's country, but not through protraction.
>
> Sun Tzu, Planning an Offensive

The first step of analyzing the concept of computer network attack is determining where it fits in the conduct of warfare. Does computer network attack fit the definition of a weapon, armed force, or some other means of conducting warfare? What importance do these definitions hold? Addressing the second question first, Martin Libicki, a senior policy analyst at RAND, writes, "Clarifying [information warfare] is more than academic quibbling. . . sloppy thinking promotes false synecdoche" (Libicki 1995, 3). Definitions shape human perceptions of concepts and link those concepts to accepted practices. Stated more narrowly, the definition of computer network attack shapes one's perception of the concept and establishes links to what United States Air Force Major David DiCenso calls the, "accepted traditional international practice," of the law of armed conflict (DiCenso 1999, 93). DiCenso served as the Assistant Professor of Law at the United States Air Force Academy and was the designer of its cyberlaw course (Peterson 1999, 127). He recognized the importance of defining information warfare before establishing any relationship to the law. He also recognized, "There is little agreement on an accepted definition [of information warfare]" (DiCenso 1999, 86).

Information warfare and computer network attack are defined by a variety of sources. Major DiCenso notes former Air Force Chief of Staff Ronald R. Fogleman's definition of information warfare as, “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” (DiCenso 1999, 86). He also cites the National Defense University's definition of information warfare as, “aggressive use of information means to achieve national objectives. . . the sequence of actions undertaken by all sides of a conflict to destroy, degrade, and exploit the information systems of their adversaries” (DiCenso 1999, 86). Turning to military doctrine, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* defines computer network attack as, “Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves” (Chairman, Joint Chiefs of Staff 1994, 98). The purpose of understanding these definitions is to glean common themes among them; themes addressing concepts such as “means,” “weapon,” and “armed” used in the laws of armed conflict.

The dictionary offers the most basic guidance in the literal interpretation of the words “means,” “weapon,” and “armed.” “Means” has the broadest definition: “a method, course of action, or instrument by which some act can be accomplished or some end achieved” (Morris 1973, 811). Computer network attack, as described in the preceding paragraph, fits the concept of a “method” and also satisfies the requirement of achieving an end. Further clarity is achieved by looking at “weapon;” defined as, “any instrument used in combat or any means employed to get the better of the other” (Morris 1973, 1451). Even if debate exists whether computer network attack is an “instrument,”

the second half of “weapon's” definition goes back to the word “means.” Having already established computer network attack as a means, it therefore also qualifies as a weapon. Finally, the word “armed” is significant because it remains an essential ingredient of the laws of “armed” conflict. “Armed” is defined simply as “equipped with weapons” (Morris 1973, 72). Again, having established computer network attack as a weapon, militaries employing such a force would be considered armed. This exercise of words may seem trivial, but in the absence of any accepted definition of computer network attack as armed force or as a weapon it is necessary to start with basic definitions. As Martin Libicki had warned earlier, clarity is a prerequisite for drawing accurate associations. Air Force Staff Judge Advocate Richard W. Aldrich notes, however, “vocabulary does not drive the law” (Aldrich 1996, 5).

Applying law to computer network attack requires moving beyond definitions and examining the outcomes of its employment. Thomas Wingfield, in his comprehensive text, *Law of Information Conflict: National Security in Cyberspace*, states, “If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets, or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism” (Wingfield 2000, 453). Martin Libicki reduces this thought to, “[Computer network attack] is examined by asking what does it do?” (Libicki 1995, 5). Effects are the primary link between computer network attack and the laws of armed conflict. United States Air Force Brigadier General David A. Deptula in his essay, *Effects-Based Operations: Change in the Nature of Warfare*, writes, “Effects-based operations provide a useful construct on how to conduct war that

can bridge the gap between the weapons of today and the weapons of the future" (Deptula 2001, 21).

Legal professionals and information operators support the focus on effects when determining the applicability of the laws of armed conflict to computer network attack. When asked, "Do the laws of armed conflict apply to computer network attack?" and "Why?" all six lawyers interviewed agreed the potential effects of such an attack warranted scrutiny under the laws of armed conflict. In a related question, "Is distinguishing 'means' of computer network attack from the 'effects' of computer network attack useful when applying the laws of armed conflict?" the six lawyers said effects were more easily analyzed while means of computer network attack were more often the source of debate on specific application of the laws. A hypothetical example provided by Charles Laedlein, Chief Legal Counsel for the Air Force Communications Agency, highlights the debate where means are concerned. His example shuts down an adversary's air traffic control system by computer network attack. Such an attack would generate the effect of reducing an adversary's capability to command, control, and detect aircraft. The attack however, is generated by transiting information technology infrastructure located in a neutral country. The laws of armed conflict specifically address the role and exploitation of neutral nations and therefore the means are also relevant to specific applications of computer network attack (Laedlein Interview, 5 March 2002). For the purpose of this thesis, potential effects sufficiently link computer network attack to the laws of armed conflict.

Laws and Cyberlaws of Armed Conflict

Computer network attack is subject to the laws of armed conflict based on the definitions discussed above and the premise that effects are a relevant consideration for the application of the laws. Part III of the 1977 Geneva Protocol I directly links the definition of computer network attack to the law. In Section I, Methods and Means of Warfare, Article 36, New Weapons, the protocol states, "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in all or some circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party" (Protocol Additional to the Geneva Conventions 1977, Part III, Section I, Article 36). Computer network attack was shown previously to satisfy the definitions of "weapon" and "means," therefore, the protocol dictates a nation examine such an attack's employment. Remembering Aldrich's admonition that words alone do not dictate law, the linkage must now be extended to effects.

The 1977 Geneva Protocol I in Part IV, Section I, General Protection Against Effects of Hostilities, Article 48, Basic Rule, also says "Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly direct their operations only against military objectives" (Protocol Additional to the Geneva Conventions 1977, Part IV, Section I, Article 48). This statement directly addresses effects without regard for the means of the "operations." Article 57 of the protocol, Precautions Against Attack, goes on to say, "Those who plan or decide upon an attack shall refrain from deciding to launch

any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (Protocol Additional to the Geneva Conventions 1977, Article 57). These two articles address the four underlying principles of laws of armed conflict introduced in chapter 1 of the thesis; military necessity, humanity or unnecessary suffering, proportionality, and discrimination or distinction. Thomas Wingfield uses these same principles and provides useful analogies for computer network attack.

Four Timeless Principles of the Laws of Armed Conflict

Military Necessity

Thomas Wingfield relates the principles of military necessity, unnecessary suffering, proportionality, and discrimination to information operations. His analogy for military necessity describes shooting down an aircraft (Wingfield 2000, 153). Wingfield argues an aircraft brought down by electro-magnetic pulse gives the pilot an opportunity to eject that he might otherwise not have had if a missile physically destroyed the aircraft (Wingfield 2000, 153). Computer network attack offers similar capabilities if we look at the power plant scenario introduced in chapter 1. Information operators could shut down a power generating facility by modifying computer code as an alternative to physically damaging the plant. Viewed from the extremes, computer network attack may save every life at the power plant while physical destruction potentially kills all humans present in the facility at the time of attack. This analogy helps identify what Wingfield calls weapons that distinguish equipment from humans (Wingfield 2000, 153). Such a distinction is useful when remembering the definition of military necessity allows, "only

that degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources" (Wingfield 2000, 148). Computer network attack, as a weapon directly targeted against equipment, "minimizes resources" while achieving its effects. Outcomes of computer network attack go beyond the immediate direct effects and therefore other principles must be examined.

Humanity, Unnecessary Suffering, and Chivalry

The principle of humanity, unnecessary suffering, or chivalry combines both quantitative and qualitative qualities of warfare (Wingfield 2000, 153). Addressing the qualitative aspects first, unnecessary suffering is caused by weapons whose effects are viewed with, "broad public antipathy," and include biological and chemical weapons and landmines (Wingfield 2000, 152). Additionally, indiscriminate effects characterize these weapons. Indiscriminate effects target no specific individual or thing. They cause destruction beyond the control of the attacker. Wingfield demonstrates the qualitative aspect of unnecessary suffering with the analogy of using clear plastic bullets. Munitions undetectable to x-ray or the naked eye could complicate an injured combatant's medical treatment and endanger the medical personnel administering care. The Geneva Convention of 1949 gives medical personnel protected status and therefore the use of clear plastic bullets fails to identify their special status (Roberts and Guelff 1982, 180). The immediate damage by the bullet is no different then an ordinary one, however the secondary effects might cause the aforementioned "broad public apathy." According to this analogy, before employing computer network attack, a combatant should consider if any indiscriminate effects could occur. Direct effects will most likely be measurable and

more immediate. Beyond the initial damage, effects' impacts will take on a more qualitative character. These secondary and tertiary effects will develop more slowly and may be more difficult to measure. The shut down, by computer network attack, of a power plant supplying electricity to a military command center may produce the desired immediate effect. If, however, other enemy power plants are used to replace the lost electricity, overloading their capacity and shutting down entire sections of a power grid, hospitals may now be affected and the consequences slowly erode public support for the method of attack. The next and more quantifiable considerations are deception and quantity of force.

Unnecessary suffering's quantifiable characteristics include perfidy and the amount of force used. Deception in warfare is a legitimate means of using force, however, deception based on violating "moral duty" or a "breach of faith" constitutes perfidy (Wingfield 2000, 165) and creates unnecessary suffering. Examples include feigning surrender, using the Red Cross symbol to gain advantage for combat, and misleading an enemy with news of a cease-fire when none exists (Wingfield 2000, 165). Similarly, computer network attack that leads an enemy to believe information came from an organization granted protected status such as the Red Cross would violate the laws of armed conflict. Permissible ruses are listed in United States Army Field Manual 27-10, *The Laws of Land Warfare*, and include, "surprises, ambushes, feigning attacks. . . transmitting false or misleading radio or telephone messages, making use of the enemy's signals and passwords, pretending to communicate with troops or reinforcements which have no existence, [and]. . . deliberate planting of false information" (Wingfield 2000, 166). Wingfield suggests that any use of computer network attack must be analogous to

established permissible ruses in warfare. Computer network attack that would mislead a power plant's crew into believing they were operating at normal capacity when in reality output was reduced causing outages is a permissible ruse following the examples of Field Manual 27-10. Unnecessary suffering's final quantifiable characteristic is the quantity of forced used.

The force, over and above that which is required to achieve an effect, is considered unnecessary. Unnecessary suffering occurs when the quantity of force crosses, in Wingfield's words, "the free floating threshold of military necessity" (Wingfield 2000,150). Using Wingfield's aircraft shoot down analogy once more, an adversary might choose between an electro-magnetic or physical means of destroying the aircraft. A belligerent choosing physical means, knowing the pilot is more likely to die, may cross the threshold of necessity and thereby cause unnecessary suffering. The key to drawing such a line is determining the target and the amount of force required to achieve the desired effect against the target. Is the target the aircraft, the pilot, or both? Targeting also proves vital to the law of armed conflict's last two principles of proportionality and discrimination.

Proportionality

Proportionality requires an attacker to weigh the value of a lawful target against probable collateral damage including civilians and civilian property (Wingfield 2000, 154-155). An attack causing excessive civilian loss of life relative to the value of the military target struck is a violation of the principle of proportionality. Thus, "As the value of a potential target increases, so does the level of permissible collateral damage" (Wingfield 2000, 155). Professor Michael Schmitt, a former faculty member at the Naval

War College, lists one of the leading causes of violating the principle of proportionality as, “a lack of full knowledge as to what is being hit” (Wingfield 2000, 115, 158). Wingfield reinforces this thought with an analogy to cyberspace where he says, “the difference between the power distribution codes for an early warning radar and an intensive care unit may be no more than a few ones and zeros in the same computer” (Wingfield 2000, 159). He continues, “The principle of proportionality in cyberspace may call for a fidelity and granularity of intelligence collection and analysis beyond current demonstrated capabilities” (Wingfield 2000, 159). Such granularity is necessary to meet the demands of discrimination.

Discrimination

Computer network attack introduces new challenges to the principle of discrimination. Discrimination separates combatants from noncombatants. The United States Navy Commander's Handbook states, “Discrimination is the customary rule of international law, which requires that belligerents distinguish between combatants and noncombatants, avoid targeting civilians and their property, and take all reasonable precautions against injuring civilians or damaging their property in the course of striking military targets” (Wingfield 2000, 140). Computer network attack will most likely rely on a dual use infrastructure: one used by both civilian society and their military (Wingfield 2000, 146). Attacks via dual use infrastructures lead to potential unforeseen effects against the civilian populace. A stand-alone computer used exclusively for military purposes represents the case for easiest identification as a military target and thus discrimination is clear. A system of systems, such as digital telephone switching center, through which both commercial and military telephone circuits run, presents a much

more complex target. Only portions of this target support military use and therefore discrimination is much more difficult.

The key, according to Wingfield, is precisely identifying, "which computers, or indeed, which programs within computers are lawful targets" (Wingfield 2000, 147-148). A useful analogy when considering dual use systems is that of placing civilians near lawful military targets or placing those same military targets within civilian structures. The use of Iraqi civilians to shield military sites from air attack in recent years is an example of this concept (Wingfield 2000, 146). The 1977 Geneva Protocol I, Article 58 makes this type of action unlawful. The article states, "The Parties to the conflict shall, to the maximum extent feasible, (a) endeavor to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives" (Protocol Additional to the Geneva Conventions 1977, Article 58). Using this analogy, a computer system or program placed deliberately within the infrastructure supporting a civilian populace is a violation of the Geneva Protocol I and renders such a computer or program subject to attack within the confines of the other principles of armed conflict. Information operators must analyze "finely sifted intelligence" to comply with the principle of discrimination (Wingfield 2000, 147).

These analogies bridge the gap between the physical world of traditional armed force and the cyber world of computer network attack. They rely on known and customary practices and show how computer network attack may be used or restrained in the conduct of war. These analogies also show the complexity of employing computer network attack and the requirement for more detailed intelligence about an enemy's systems. Finally, the infancy of computer network attack and its rapidly changing

capabilities will require information operators to establish effective relationships with their associated legal counsel. Compliance with law ultimately serves national interests. Responsibility of command dictates adherence to the law at personal and organizational levels.

The Accountability of Command

Role of the Commander

Commanders accept the responsibility for decision making and are accountable for the outcomes of their decisions. Commanders of 21st Century information warfare organizations will make decisions on the employment of computer network attack. Ensuring those decisions comply with the law is inherently the responsibility of the commander. Joint Publication 3-13, *Joint Doctrine for Information Operations*, says "The growth in IO-related technologies and capabilities and associated legal issues makes it critical for commanders at all levels of command to involve their staff judge advocates in development of IO plans and conduct of IO" (Chairman, Joint Chiefs of Staff 1998, I-5). Lieutenant Colonel Joe Dhillon, a member of United States Space Command's staff judge advocate staff, clarified this relationship in an interview when he was asked what is the role of legal counsel in the application of computer network attack? Lieutenant Colonel Dhillon emphasized that though the staff judge advocate provides legal counsel on the employment of computer network attack, ultimately the decision and consequence of employment rests with the commander (Dhillon Interview, 19 March 2002). This thought is echoed by United States Air Force Colonel David L. Goldfein in his book, *Sharing Success Owning Failure: Preparing to Command in the Twenty-First Century Air Force*. Colonel Goldfein writes, "In working with [lawyers] , the best advice to

remember is as follows: Lawyers are responsible for the law, but commanders are responsible for justice" (Goldfein 2001, 80). Additionally, commanders rarely employ force as a lone individual.

Force is executed by applying joint and service doctrine normally through the command of people. Doctrine guides the implementation of force. In the case of information operations, Joint Publication 3-13 tells the commander he, "must understand the different legal limitations that may be placed on IO across the range of military operations" (Chairman, Joint Chiefs of Staff 1998, I-1). Once an understanding of the law is obtained the commander must act on that knowledge. The United States Army's Command and General Staff College Student Text 27-1, *Military Law*, defines command responsibility concerning the laws of armed conflict. The text states, "Commanders are also obligated to (1) ensure subordinates are trained regarding their responsibilities under the law of war; (2) enforce proper rules of engagement; and (3) issue clear, unambiguous, and lawful orders" (Chairman, Joint Chiefs of Staff 25 March 2002). This command relationship rests on a clear chain of command and the concept of lawful orders.

Lawful Orders

Military members will execute computer information attack based on the lawful orders of their superiors. The Manual for Courts-Martial defines a lawful order as a directive given within the limit of a superior's authority, related to military duty, morale, or discipline, clear and unequivocal, and received and understood (Manual for Courts-Martial 2000, IV-19). Superiors bear no greater burden in proving an order concerning computer network attack is related to military duty, morale, and discipline than in any other use of force. A superior's additional burden, where computer network attack is

concerned, is clarity both at the issuing and receiving ends of an order. Clarity and understanding when ordering computer network attack assumes both the ordering and receiving individual are sufficiently trained in the methods of computer network attack and the legality of those methods in terms of expected outcomes. As shown previously, discrimination is required by the laws of armed conflict; therefore, information operators must be fully trained in the intricacies of computer network attack methods and not just in the initial keyboard commands required to execute the attack. A computer network attack operator will only be in receipt of a lawful order when he or she clearly understands the method of attack and that the method was scrutinized and found consistent with the principles of the laws of armed conflict. Military members, commanders and subordinates, ultimately base their judgement on whether an order is lawful through their understanding of what the law requires.

Authority and Organizational Structure

Information operators employing computer network attack must also ensure orders from superiors are given within that superior's authority. Authority is derived from “law, regulation, or custom of the service” (Manual for Courts-Martial 2000, IV-19). The foundation for authority is established by commissioning of officers, appointment to command, and the subsequent organization and manning of positions within an organization. Additionally, an organization's mission statement and the duties and responsibilities given to its leaders help form the basis of authority. Information operators must understand who within their organization is vested with the authority to order computer network attack and how that authority is relayed to the attacker.

Hierarchies are established both within an organization and between organizations. The relationship between organizations is also key to the issue of authority.

Governance or rules enable organizations within a greater corporate structure to operate effectively (Strassmann 1995, 38). Paul Strassmann, the former Director of Defense Information and visiting professor of information warfare at the National Defense University, says, "An organization can either sanction some measures of control through formal rules of corporate governance, or abandon such an idea in favor of just about everybody pursuing autonomous initiatives. Where a power vacuum exists, [leaders] will seek to assert their own initiatives" (Strassmann 1995, 38). Corporate structures that desire to avoid the "pursuit of autonomous initiatives" should create clear missions for each level of organization and define authority relationships between those organizations. The United States Air Force follows the above concept when it establishes levels of command such as major commands, numbered air forces, wings, and squadrons and gives each specific missions. These organizations are guided further by Department of Defense and service policies and regulations governing those missions.

Given the reasoning above, one would expect the Department of Defense to assign the mission of computer network attack and create the necessary organizational structure to carry out the mission. A second expectation is that the Department of Defense would create lines of authority for computer network attack by establishing command relationships between those same organizations. Finally, the Department of Defense should establish some form of governance for computer network attack organizations and that governance should address how those organizations should apply the laws of armed conflict to computer network attack. These are not new ideas. A 1996

RAND issue paper, *Information War and the Air Force: Wave of the Future? Current Fad?*, called for establishing national policy in the area of information warfare by, "defining the national interest, establishing a mechanism for setting priorities among competing objectives, and assigning responsibility for enforcement" (Buchan 1996, 16). Absent these three conditions, one could reasonably expect computer network attack organizations to apply the laws of armed conflict based on their own initiatives resulting in inconsistencies. Clearly established command relationships and policies aid in determining lawful orders. The next step is ensuring those orders are based on sound knowledge of the law.

A construct for applying laws of armed conflict to computer network attack is needed to satisfy the requirements of the law, responsibilities of command, and to ensure consistency within the Department of Defense. Computer network attack by definition and potential effect on an adversary subjects itself to the scrutiny of the laws of armed conflict. Additionally, commanders are obligated to ensure they personally follow the guidelines of law and train their subordinates to understand the law's requirements. Finally, the chain of command and clear organizational structure clarify the concept of lawful orders. The requirement for a framework of law addressing computer network attack is established. The next question is whether such a framework exists.

A Legal Framework for Computer Network Attack: Myth or Reality?

Early Research

The first round of interviews with lawyers and information operators produced no evidence of standard or unique frameworks of law related to computer network attack. Each of the legal counselors interviewed shared the belief that the potential use of

computer network attack was reviewed for legality on a “case-by-case” basis. The question was also asked if information operators were trained on the laws of armed conflict as it relates to computer network attack? All four information operators interviewed answered in the affirmative. When asked to describe the training each individual acknowledged the lesson as a standard law of armed conflict briefing tailored by the trainer to information operations. The lawyers' response mirrored that of their pupils. The lawyers were then asked if they ever cross-flowed training materials or made any effort to standardize law of armed conflict training specifically tailored for information operations? The answer was no. Colonel Dhillon told of legal conferences and workshops conducted to address the issue of information operations and the law. In the end, however, he conceded that no specific product relating law to information operations was produced as a result of those conferences (Dhillon Interview, 19 March 2002). Without evidence of a standard framework of law for computer network attack, this thesis was prepared to argue what such a framework might resemble. The argument became unnecessary when another information operator, Richard Moore of the Joint Information Operations Center, revealed the work of Thomas Wingfield.

Discovery

Thomas C. Wingfield's *Law of Information Conflict: National Security in Cyberspace* is the only scholarly work relating law to computer network attack. The text is comprehensive in its coverage and shares the same conclusions made in the early drafts of this thesis. In fact, the eleven chapter text went well beyond the depth of this thesis. Original thoughts and analysis of earlier drafts that mirror in any way the writings of Mr. Wingfield are now attributed to his text to avoid any perception of plagiarism. By

exploring Wingfield's work the thesis will show the essential parts of an existing framework of analysis for computer network attack. Once explored, the second piece of the primary question is asked, "Is the framework applied by information operators charged with executing computer network attack?"

A Framework Exists

Thomas Wingfield introduces a framework of analysis for computer network attack based on the work of Michael N. Schmitt, a former faculty member at the United States Naval War College. The framework evaluates, "the quantitative consequences of a proposed information operation in terms of the qualitative criteria that distinguish military force from diplomatic or economic coercion" (Wingfield 2000, 119). Information operators are given six criteria, developed by Schmitt, to analyze potential uses of computer network attack. These criteria are: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy (Wingfield 2000, 119).

A brief description of each of the criteria is provided below and is also shown in figure 3. Severity examines the physical destruction in terms of numbers of people killed, the area or scope of the attack, and the amount of damage done or intensity (Wingfield 2000, 120 and 124). Immediacy looks at the total time required from attack initiation to the observation of the effect. It also considers how long the effect will last (Wingfield 2000, 120 and 124). Directness considers whether the means of attack was distinguishable from other "parallel or competing actions" and also if the attack is attributable to the resulting effect (Wingfield 2000, 120 and 124). Invasiveness determines whether the means of attack crossed the territorial borders of the nation

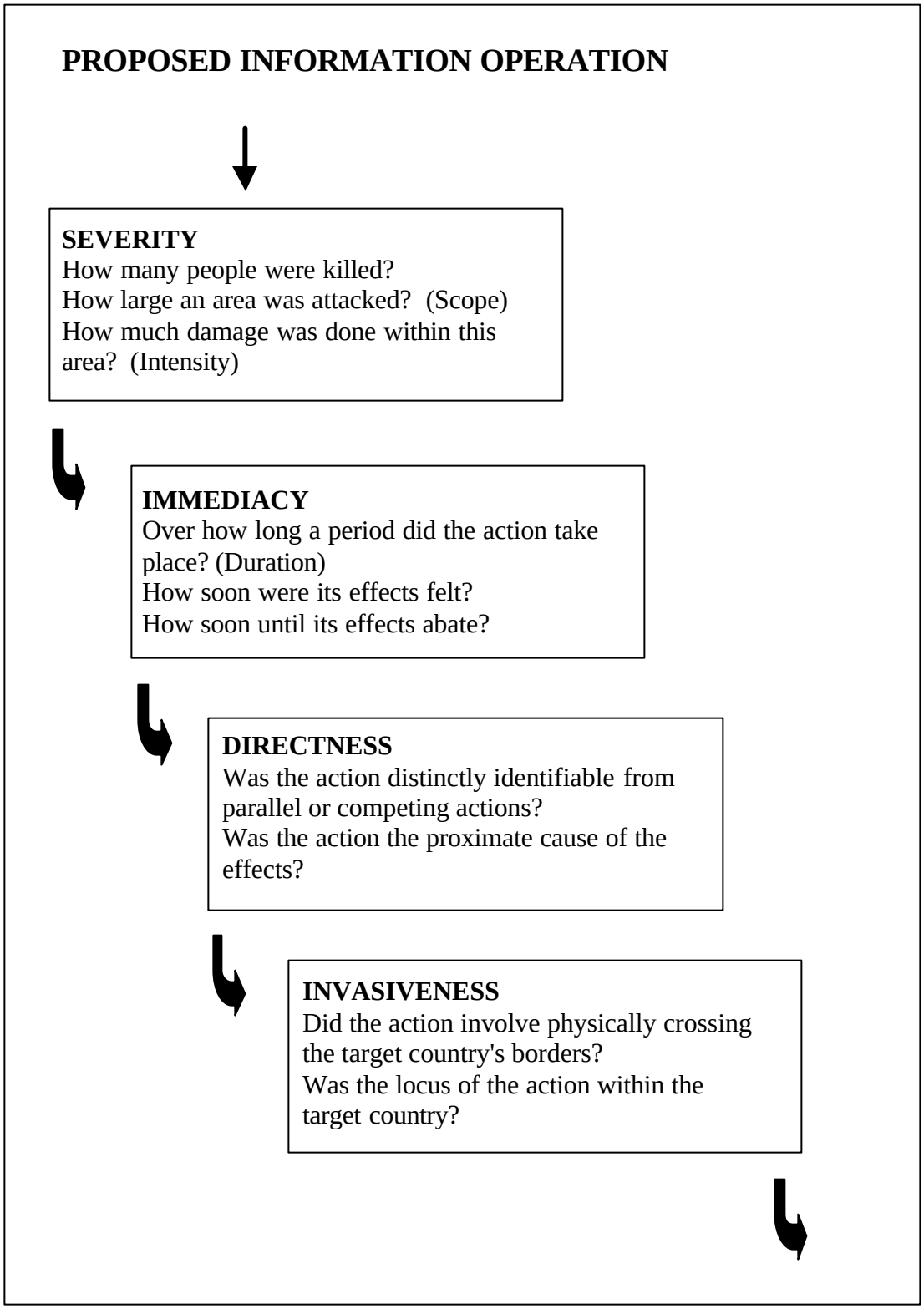

Figure 3. The Schmitt Use of Force Analysis (Wingfield 2000, 124)

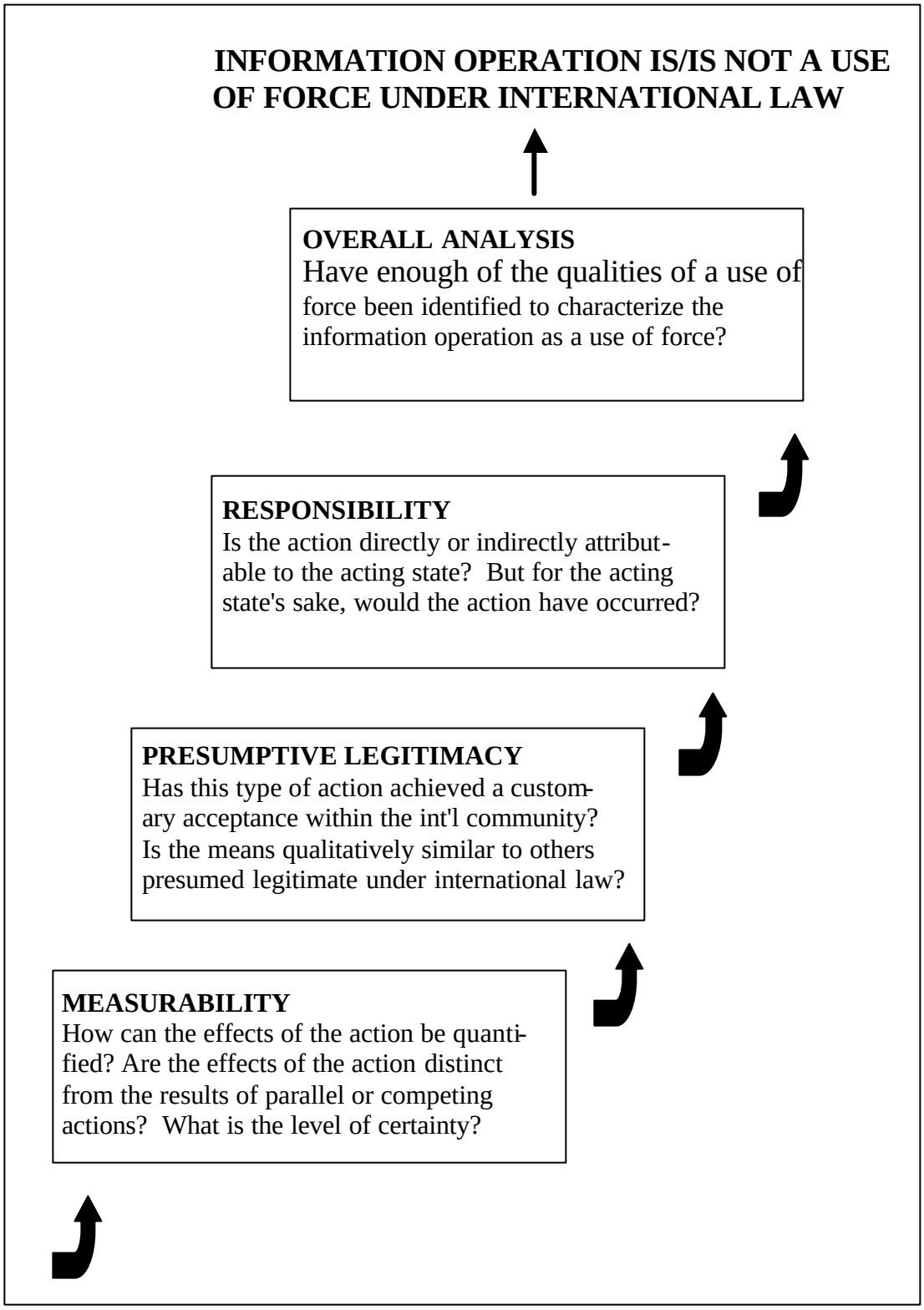

Figure 3. continued (Wingfield 2000, 125)

targeted (Wingfield 2000, 121 and 124). Measurability requires the effects be quantified. It also seeks to distinguish the quantifiable effects of one weapon from other means used in levels of certainty (Wingfield 2000, 121 and 125). Finally, presumptive legitimacy looks at whether computer network attack's effects are, "qualitatively similar to others presumed legitimate under international law" (Wingfield 2000, 121 and 125).

The goals of this framework are twofold: "first, [computer network attack's] real-world destructiveness would form the basis of the decision of whether or not to carry it out, and second these consequences would be expressed in such way as to bring the analysis in line with the [United Nations] Charter drafters' principled distinction between military and other forms of coercion" (Wingfield 2000, 120). This distinction is important to the framework. In the past the United Nations Charter evaluated coercive power only by asking if military force was used (Wingfield 2000, 119). The Schmitt analysis takes the distinction one step further by assessing, "the consequences that have resulted" (Wingfield 2000, 119).

This Schmitt analysis suggests the military use of computer network attack could be used both above and below the threshold of force defined by Article 2 (4) of the United Nations Charter. A military could use the framework to establish where computer network attack fell on the spectrum of force. Figure 4 shows each of the criteria at three different levels of that spectrum. But is the framework useful for analyzing computer network attack in terms of the laws of armed conflict above the Article 2 (4) threshold? The framework is missing the link of each of these criteria to the four general principles of military necessity, unnecessary suffering, proportionality, and discrimination.

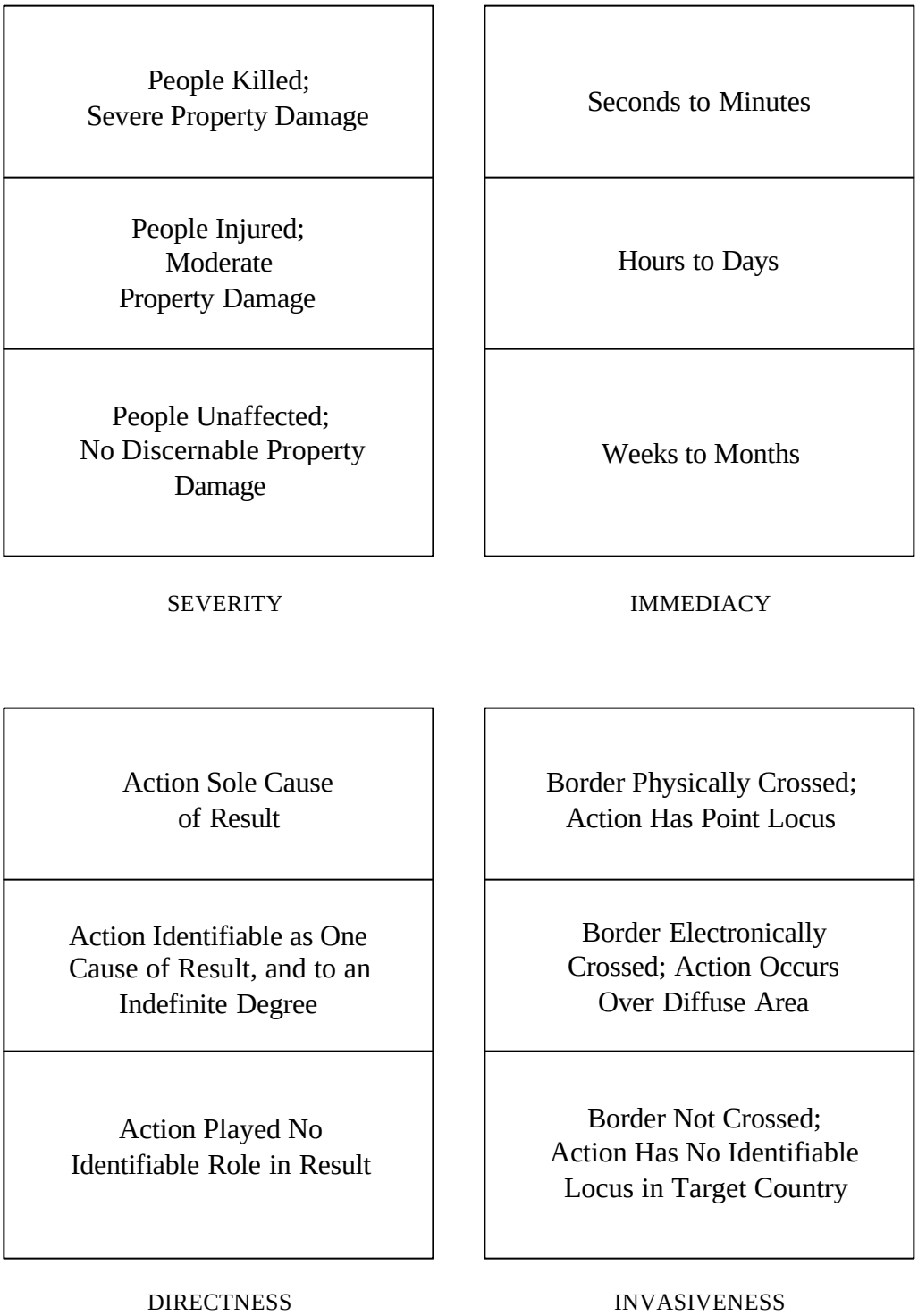

Figure 4. Schmitt Analysis Factors (Wingfield 2000, 126)

Figure 4. continued (Wingfield 2000, 127)

Elements of the criteria directly lend themselves to such a correlation. For example, the criterion of immediacy discusses the length of effects which potentially addresses the principle of unnecessary suffering. Measurability characteristics of quantifiable results could aid determination of proportionality. Without these links to the four general principles the framework can only be used to decide whether *jus ad bello*, the body of laws appropriate before armed conflict, or *jus in bello*, the laws of armed conflict, are applied to computer network attack.

Tool or Vision?

The existence of a framework satisfies only half of the primary endeavor of the thesis. The remaining proof, and perhaps most important, was whether the framework of law, developed by Schmitt and presented by Wingfield, was used in the field. Initial research led to the conclusion such a construct was not in use. Rather than rely on earlier research and interviews to draw conclusions, each original participant was contacted again by phone or e-mail and asked if they knew of Thomas Wingfield's text and whether the text was used in any manner to apply laws of armed conflict to computer network attack. Three of the original eight participants responded they were aware of the book; two lawyers and one information operator. Only Richard Moore, at the Joint Information Operations Center, was aware of attempts to codify the Schmitt analysis into the processes of Department of Defense information operations. Moore developed a software program automating the question flow shown in figures 3 and 4. This software, according to Moore, will be included in a future version of the Joint Operation Planning and Execution System's (JOPES) planning software suite (Moore interview, 22 April 02). JOPES is the, “integrated joint conventional and nuclear command and control system

used to support military operation planning, execution, and monitoring activities" (United States Transportation Command 2000, 1-10). He was also aware of the introduction of Schmitt's analysis to the students attending Air Force Special Operations Command's Information Operations Planners Course (Moore Interview, 22 April 2002). Captain Tyler Moore, one of the course instructors, confirmed this fact (Moore Interview, 28 April 2002). Finally, the most conclusive evidence was an interview with Thomas Wingfield. He said the Schmitt framework was used but agreed that perhaps only "10 to 20 percent" of information operations organizations were aware of its utility (Wingfield interview, 29 April 2002). If these are the only applications of Schmitt's framework, why are other efforts to either use Schmitt's work or any other framework not underway? What are the current hurdles to such efforts?

The Application of Law to Computer Network Attack: Organizational Constraints

Doctrinal Guidance

Organizational structures and the relationship of the legal and information operations communities pose challenges to adopting and using a standard framework of analysis for applying law to computer network attack. Doctrine provides a map for organizing information operations. Joint Publication 3-13, *Joint Doctrine for Information Operations,* addresses, "IO principles relating to both offensive and defensive IO, and describes responsibilities for planning, coordinating, integrating, and deconflicting Joint IO" (Chairman, Joint Chiefs of Staff 1998, i). The publication also states, "Offensive IO may be conducted at all levels of war--strategic, operational, and tactical--throughout the battlespace" (Chairman, Joint Chiefs of Staff 1998, viii). These two statements suggest a clear organizational structure and chain of command, from strategic levels through

tactical execution, is needed to carry out the planning, coordination, and deconfliction of offensive IO. The same conclusion was shown in arguing what was needed for lawful orders in the implementation of computer network attack. The publication outlines the responsibilities of key participants to include the Chairman, Joint Chiefs of Staff, the combatant commanders, service chiefs, Director of the Defense Information Systems Agency, Director of the Joint Command and Control Warfare Center (now the Joint Information Operations Center), and several other intelligence directorates and agencie (Chairman, Joint Chiefs of Staff 1998, I-6 - I-8). Specific guidance concerning organizational structure and relationships, however, is limited to the service chiefs. They are directed, "To maintain liaison with Services, Defense agencies, and other appropriate agencies to minimize duplication of capabilities" (Chairman, Joint Chiefs of Staff 1998, I-7). Current joint doctrine outlines what the map should achieve, but it relies on the services to create the necessary organizational infrastructure.

A Service's Structure for Information Operations

Service controlled information operations and the existence of several joint agencies resulted in unsynchronized information operations capabilities. Maintaining a liaison merely to avoid overlap did little to encourage synergies among the various players. Keeping in mind the benefits of a clear chain of command and organizational structure discussed previously, the conditions were ripe for inconsistent application of law to computer network attack. Looking at the Air Force information operations structure as of 1999 in figure 5 shows why.

The Air Force information operations organizational structure, similar to other service structures, was fragmented. The number of agencies and directorates and their

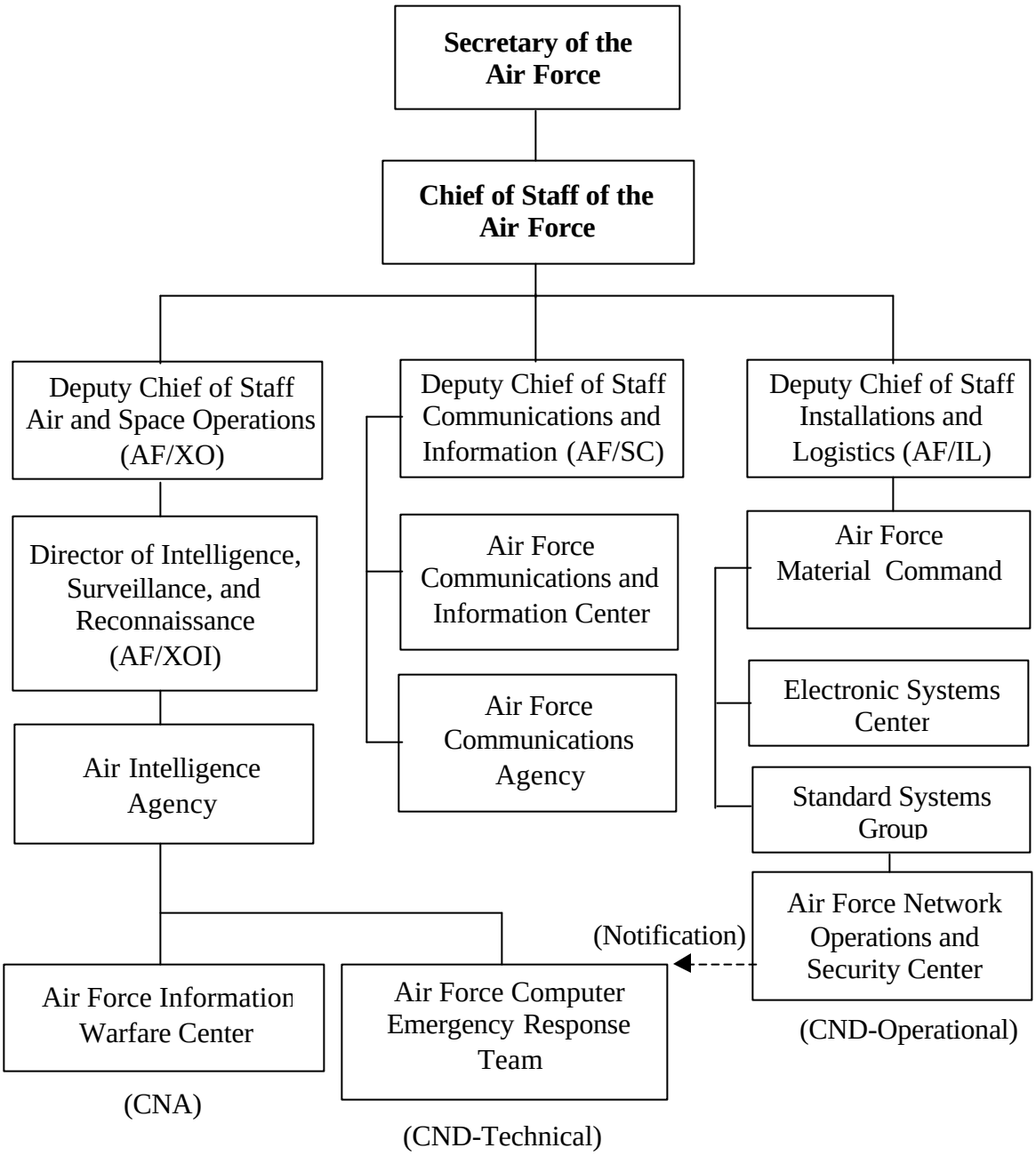

Figure 5. Air Force Information Operations Structure 1999

competing chains of command eroded potential synergies. Headquarters Air Force Communications and Information Directorate at the Pentagon wrote policy for information technology and budgeted for its implementation. The Air Force Communications Agency at Scott Air Force Base, Illinois, assisted in this effort but was also responsible for evaluating commercial off-the-shelf information technology and executing policy by standardizing information technology used by the Air Force. Both organizations focused on the defensive aspects of information operation (Chairman, Joint Chiefs of Staff 1999, A-53). The Electronic Systems Center at Hanscom Air Force Base, Massachusetts, and the Standard Systems Group at Gunter Air Force Base, Alabama developed software and systems to support the policy writers but fell under a completely different chain of command (Chairman, Joint Chiefs of Staff 1999, A-53). The communications directorate and the communications agency reported to the Deputy Chief of Staff Communication and Information (AF/SC) while the systems center and group reported to the Deputy Chief of Staff Installations and Logistics (AF/IL) (Chairman, Joint Chiefs of Staff 1999, A-50).

Further, the information operators resided at the Air Intelligence Agency's Air Force Information Warfare Center. These two organizations focused primarily on the offensive portions of information operations but also retained the service's defensive oriented computer emergency response teams (Air Force Information Warfare Center 15 March 2002 and Department of the Air Force, Headquarters Air Intelligence Agency 1 May 1998). The Air Intelligence Agency reported to the Director of Intelligence, Surveillance, and Reconnaissance (AF/XOI) and Deputy Chief of Staff Air and Space Operations (AF/XO) respectively (Chairman, Joint Chiefs of Staff 1999, A-52). All

worked toward improving information operations but faced the challenge of geographic separation, stove-piped chains of command, and competing budget and policy issues. In the year 2001 the Air Force seems to have made the situation worse (see figure 6).

The realignment of the Air Intelligence Agency from the Director of Intelligence, Surveillance, and Reconnaissance to Eighth Air Force on 1 February 2001 shifted information operations from a functionally oriented to a geographically oriented organization (Air Combat Command News Service, 26 October 2000). Numbered air forces are, "the senior warfighting echelon of the US Air Force," and are normally geographically aligned with the geographic combatant commands (Headquarters Air Force Doctrine Center 2000, 34). The new information operations mission requires Eighth Air Force to expand their role beyond their normal geographic orientation to support all other combatant commanders. Colonel Carla D. Bass, former commander of the 694th Intelligence Group, Air Intelligence Agency, notes, "Organizing information operations functionally. . . capitalizes on three long-held military principles. . . unity of command. . . mass. . . and economy of force" (Bass 1999, 36).

Air Force doctrine explains, "Unity of command ensures the concentration of effort for every objective under one responsible commander" (Headquarters Air Force Doctrine Center 1997, 12). According to Colonel Bass the lack of unity of effort for information operations has resulted in, "uncoordinated and unevenly focused [efforts] across the defensive and offensive facets of information operations" (Bass 1999, 36). Multiple commanders result in multiple priorities and each commander competes over scarce resources eroding computer network attack's potential (Bass 1999, 36). Her views are echoed by Colonel James M. McCarl, the commander of the United States Army's

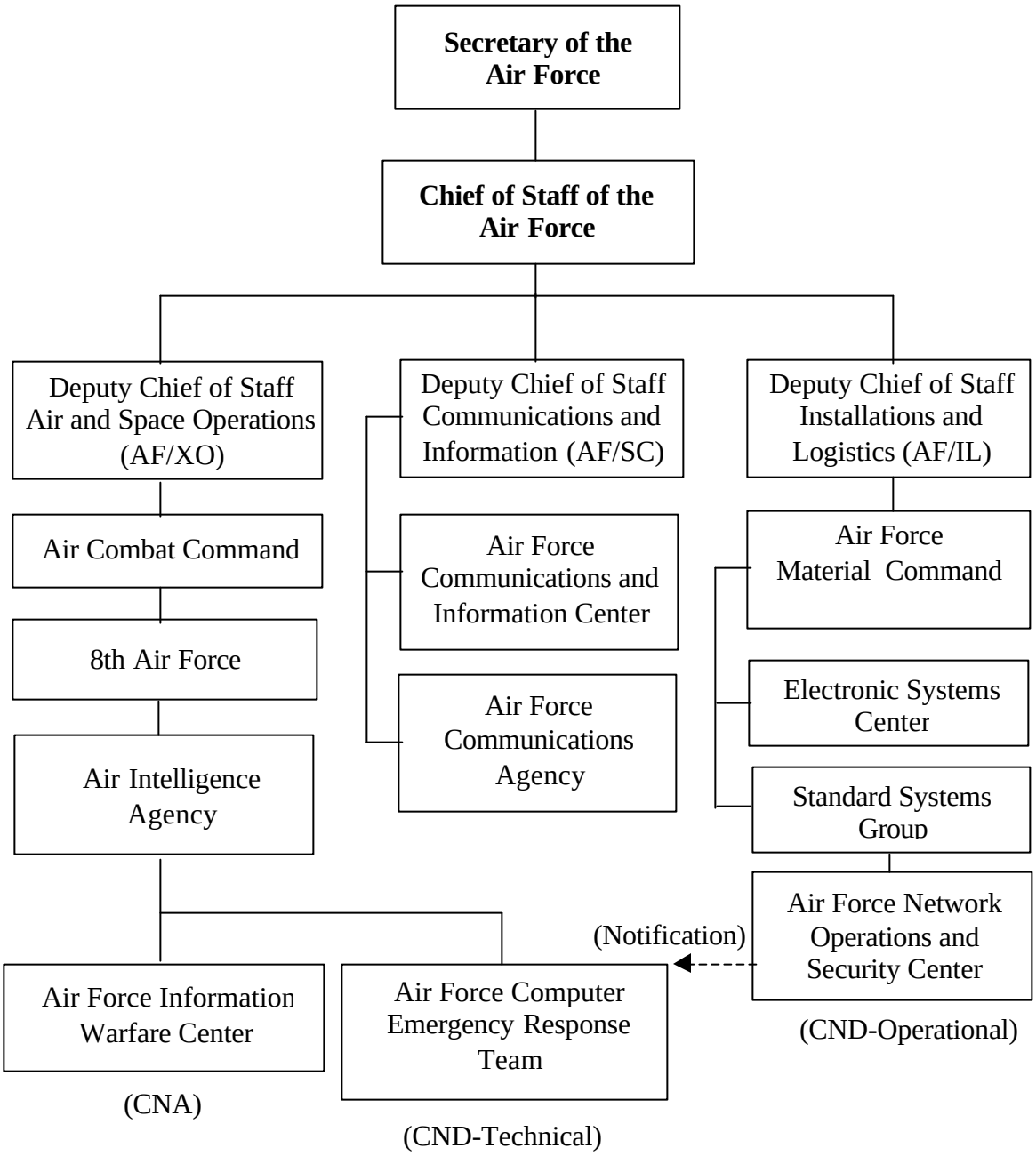

Figure 6. Air Force Information Operations Structure 2002

Land Information Warfare Activity (LIWA). Colonel McCarl stated, “The solution may be to place information operations entirely under one commander in chief in the same manner that an air war is guided by its own commander” (Ackerman March 2002, 26).

The second principle, mass, calls for, “concentrating combat power at a decisive time and place” (Headquarters Air Force Doctrine Center 1997, 13). This principle is based on efficiency (Headquarters Air Force Doctrine Center 1997, 13) that is gained through the focus of a single commander toward an objective (Bass 1999, 36). Finally, to ensure force against the objective is optimized, information operators should follow the principle of economy of force. Economy of force, “[ensures] overwhelming combat power is available, [by] minimizing combat power [toward] secondary objectives” (Headquarters Air Force Doctrine Center 1997, 18). Information operations leaders, using this principle, are able to, “recommend the most effective mix of information operations assets for applications in military operations” (Bass 1999, 36). Based on this evidence, perhaps the combatant commanders would have been better served if the United States Air Force had realigned its information operations mission under a functional organization such as the Air Force Space Command. The joint community is already moving in this direction.

Department of Defense Information Operations

The structure of Department of Defense information operations by the year 1999 was fragmented into offensive and defensive operations as depicted in figure 7. Examining each independently shows the challenges faced in formulating a coherent legal framework for information operations. The Defense Information Systems Agency's Global Network Operations and Security Center championed defensive information

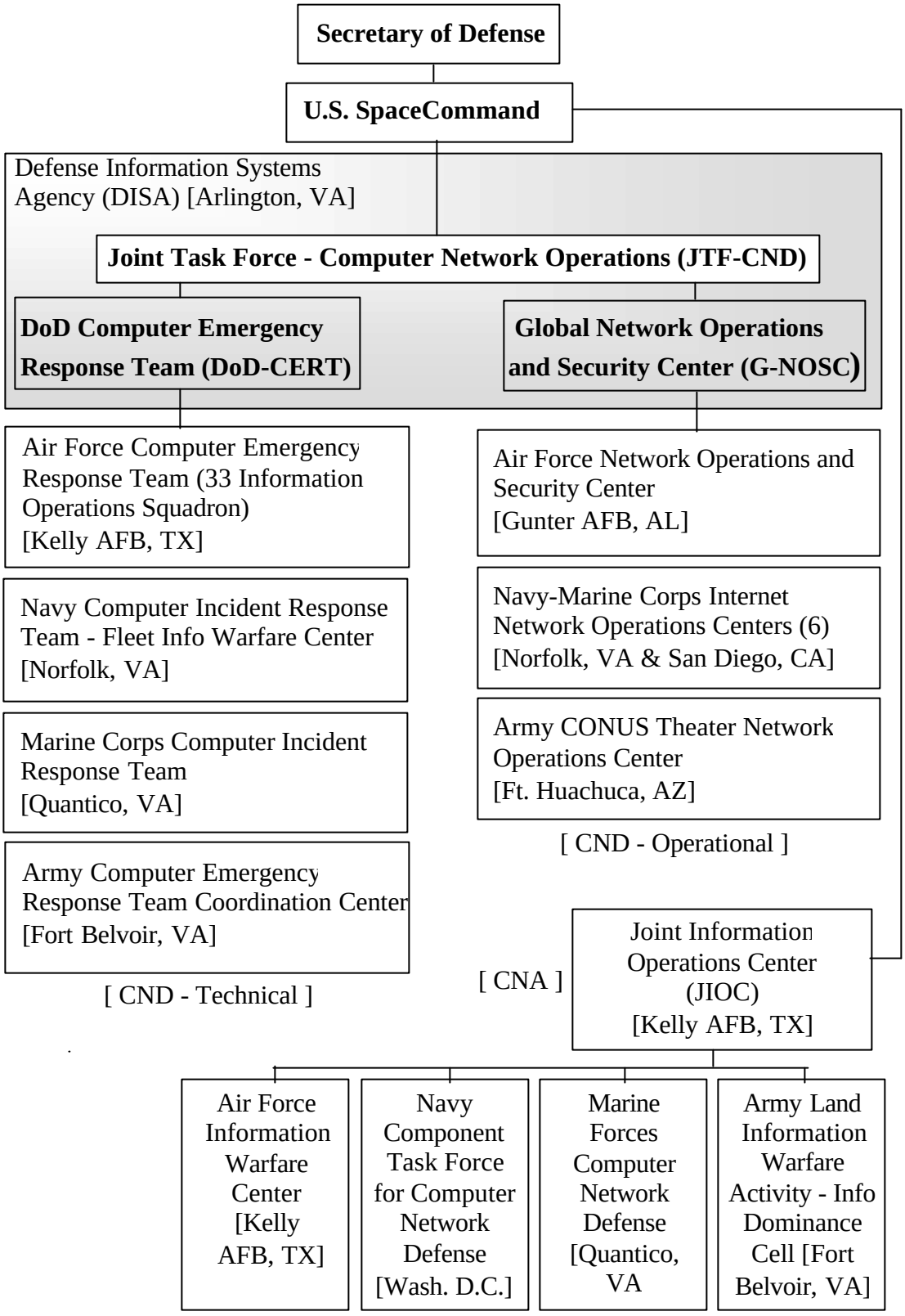

Figure 7. Department of Defense Information Operations Structure 1999

operations and Joint Task Force Computer Network Defense collocated in Arlington, Virginia (Defense Information Systems Agency 14 June 2000). They were mirrored by counterparts in each service such as the Air Force's Network Operations and Security Center at Gunter Air Force Base, Alabama. These centers were further complemented by service directorates and agencies responsible for writing policy and approving equipment to achieve "information assurance." The offense portion of information operations was the domain of "the shooters" and was provided to the combatant commanders through United States Space Command. The Joint Information Operations Center was United States Space Command's offensive information operations organization. The center creates teams oriented to support the various geographic combatant commanders. While the joint community used a functional command to support combatant commanders, the command it chose remained split in its ability to conduct coordinated offensive and defensive operations. However, this changed with the creation of the Joint Task Force Computer Network Operations.

Offense vs. Defense

Computer network defense is designed to prevent computer network attack by an adversary and therefore legal lessons learned about methods and means of those attacks are directly transferable to offensive information operations. Additionally, the high speeds at which computer network attack occurs dictate the defender have access to retaliatory capability as an active defense. Joint Publication 3-13 envisioned these concepts when it stated, "Because they are so interrelated, full integration of the offensive and defensive components of IO is essential" (Chairman, Joint Chiefs of Staff 1998, ix). The reality in 1999, however, could not have been further from the desired end state.

Anthony Cordesman, a director at the Center for Strategic and International Studies, claims that even in 2002, “There is a clear disconnect between the efforts in the U.S. to plan offensive cyber-warfare and efforts at cyber-defense” (Cordesman 2002, 3). Examination of figure 7 shows the divergent structures with little or no overlap except at the highest levels of command. Several real world threats and one test of United States vulnerabilities drove information operators toward the common goal envisioned by Joint Doctrine.

A Step in the Right Direction

The Department of Defense recently created a more proactive and unified structure for conducting information operations (see figure 8) by combining offensive and defensive capabilities into one organization. The creation of the Joint Task Force Computer Network Operations (JTF-CNO) provides the United States military with a single focal point for information operations (United States Congress, House, 17 May 2001). In his testimony to the House Armed Services Committee on May 17, 2001, the Honorable Linton Wells II, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (Acting), said, “[the JTF-CNO] answered the ‘Who's in charge?’ question” (United States Congress, House, 17 May 2001). He continued, “Prior to the formation of the JTF, no single entity had the authority to coordinate and direct a DoD-wide response to a computer network attack” (United States Congress, House, 17 May 2001). Mr. Well's assessment of information operations' organizational structure succinctly captures the result of the fragmented relationships shown previously:

> The existing [information operations] capability had been developed from the ground up to meet local or individual component requirements. Among components, there was significant variability in philosophy and approach,

> organizational and functional construct, and capability. The assessment concluded that the current independent, 'bottom up' construct had reached its potential, would soon be overcome by rapidly growing component demand, and would not scale to support the emerging urgent requirement for a unified Defense-wide capability (U.S. Congress, House, 17 May 2001).

JTF-CNO is an expansion of the Joint Task Force Computer Network Defense. The move combines computer network attack with the current network defense capabilities (Seffers 09 May 2001). The task force reports to United States Space Command, a functional command responsible for supporting all combatant commanders. United States Space Command now controls computer network attack for the Department of Defense (United States Space Command 14 December 2001). The only remaining question is what relationship the Joint Information Operations Center has with the new JTF-CNO. This new structure clarified the chain of command, brought together the defensive and offensive portions of information operations, and provided an opportunity for unified and consistent application of law to computer network attack.

The Application of Law to Computer Network Attack: Lawyer / Operator Relationships

The legal community's lack of a central plan and standards for applying laws of armed conflict to information operations and the strained relationship between lawyers and operators create a second hurdle for the consistent application of law to computer network attack. The six lawyers interviewed indicated there was no standardized training across the Department of Defense for applying law to computer network attack. Several interviews did produce evidence that training in this area is conducted disjointedly. For instance, the legal staff at the Aerospace Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance Center (AC2ISRC) at

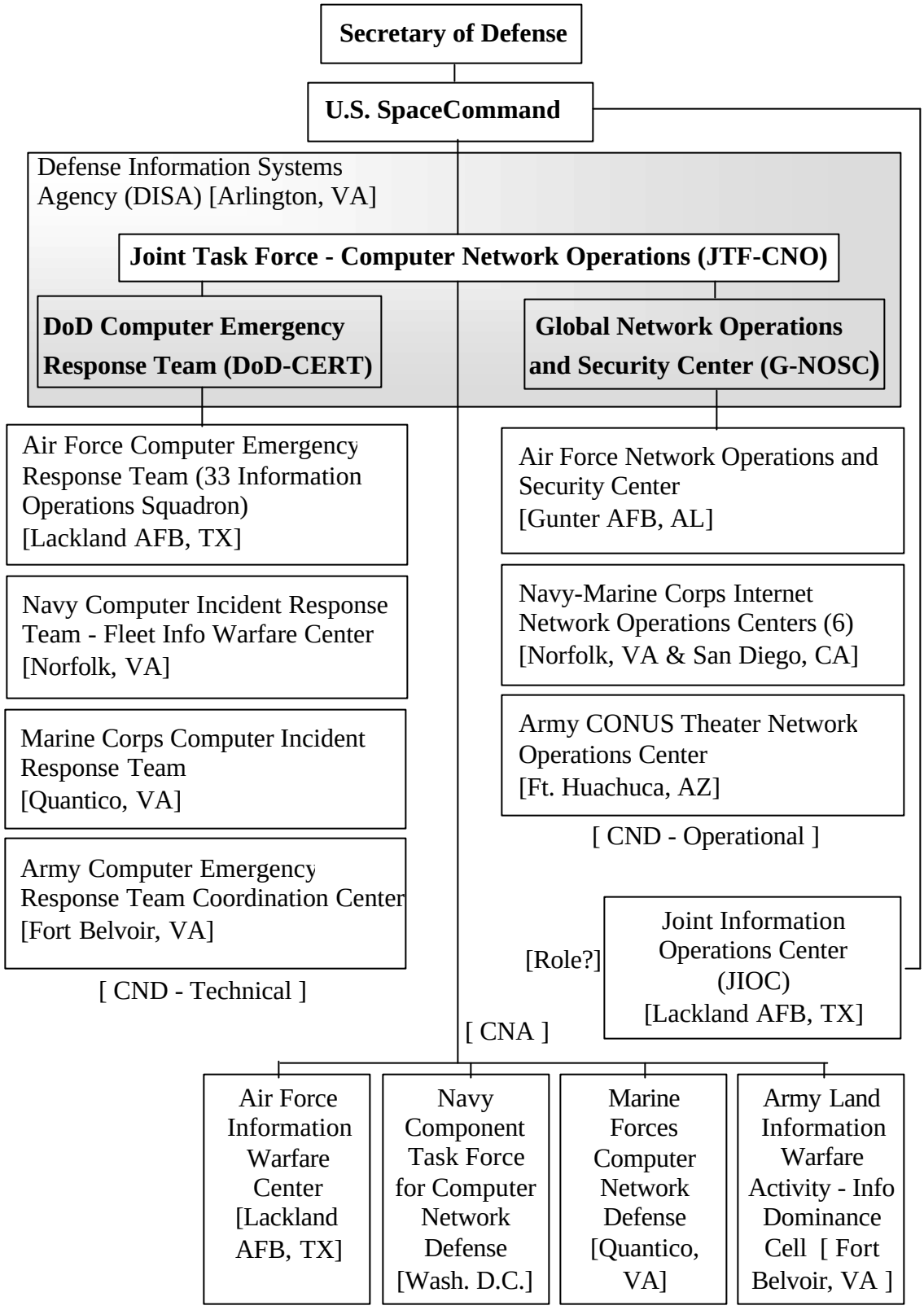

Figure 8. Department of Defense Information Operations Structure 2002

Langley Air Force Base, Virginia, conduct a course for other Department of Defense lawyers on information operations (Moore interview 22 April 2002). This course includes law of armed conflict training. This is a case of lawyers training lawyers. Similarly, the Air Force Special Operations Command at Hurlburt Air Force Base, Florida, teaches a course on information operations planning that includes a portion on the laws of armed conflict. This course is taught by qualified information operators with lawyers providing the training for the laws of armed conflict portion (Williamson interview 19 March 2002). These are the only two examples uncovered in the interviews and a search of literature that show a centralized effort to standardize training. All other training of laws of armed conflict is accomplished at the organizational level. In one case the lawyer assigned responsibility for training laws of armed conflict did not address the information operators directly. He simply gave advice to the lawyer assigned to the information operations squadron charged with the mission of computer network attack. Even when the training does occur in a centralized or decentralized fashion, the relationship of lawyers and their clients is not always a good one.

Information operators perceive lawyers as a constraint in the conduct of operations. This is an assumption, although the weight of evidence shows the assumption to be true. All interviewed subjects agreed the relationship was strained. Respondents used words such as “forced,” “awkward,” and “strained” to describe the lawyer/operator relationship. In the words of Geoffrey Best, the author of *Humanity in Warfare*, “Few bodies of trained men are more intensively trained to do what they are told to do, and *not* (Best's emphasis) to do what they have been told not to do, than professional soldiers” (Best 1980, 23). A recent report describing the strained relationship of the assistant staff

judge advocate at United States Central Command and its commander General Tommy Franks may be indicative of this relationship even at the highest levels (The Associated Press, 19 November 2001). It should be noted, however, that General Franks did not fire his lawyer as attributed in the press but rather retained the person's services because of the close relationship the lawyer had built with his staff (Williamson interview, 19 March 2002). Other methods of building teamwork-oriented relationships include sending lawyers to service and Department of Defense schools and including legal counsel in training and exercise scenarios (Williamson interview, 19 March 2002). Another area where a stronger bond between lawyer and information operator could exist is in the form of technical training.

Lawyers assigned as counsel to information operators in most cases do not have the technical training required to understand the discipline practiced by their clients (Williamson interview, 19 March 2002). Lieutenant Colonel Charlie Williamson, Chief Legal Counsel Joint Task Force Computer Network Operations, stated most military lawyers understand the basic concepts of physics and have seen bombs on airplanes or shells in tanks and can understand the consequences of their use. Few lawyers, however, understand how technology works in the process of computer network attack (Williamson interview, 19 March 2002). Williamson suggests establishing a program for lawyers similar to the Medical Law Consultant Program. This program sends lawyers to five weeks of training at major medical centers where the lawyers witness the rigors of practicing medicine. He recommends a similar program for information operations lawyers (Williamson interview, 19 March 2002). The JTF-CNO has started a similar program for its organization whereby assigned legal counselors attend three weeks of

information technology training to include network fundamentals and a course on hacking (Williamson interview, 19 March 2002). Such a program instituted at the Department of Defense or service level would help other information technology-dependent disciplines as well.

Summary

A basic framework for applying the laws of armed conflict to computer network attack exists in the form of the Schmitt Analysis. This framework however, is only sufficient for establishing whether an act of computer network attack crosses the threshold between *jus ad bello* and *jus in bello* as defined by United Nations Charter, Article 2 (4). The framework must be linked to the principles of military necessity, unnecessary suffering, proportionality, and discrimination for analysis of potential computer network attack in combat. Additionally, the framework, as it stands currently, is used in rare occasions throughout the Department of Defense. Disjointed organizational structures and a strained relationship between lawyers and information operators impede its adoption or any other attempt to standardize analysis of computer network attack.

CHAPTER 5

CONCLUSIONS

Primary Questions Revisited

Computer network attack, used by the United States military in combat, is subject to the laws of armed conflict. The systematic and consistent application of the laws of armed conflict to computer network attack requires a framework for analysis. Thomas Wingfield in his text, *The Law of Information Conflict: National Security Law in Cyberspace*, provides the beginnings for such a framework called the Schmitt analysis. Interviews with information operators and their associated legal counsel however, show that Wingfield's work is not widely known and application of the laws of armed conflict to computer network attack is not consistent throughout the Department of Defense. Evidence also shows these inconsistencies are driven by uncoordinated legal training between organizational levels and the lack of a clear organizational structure for computer network attack.

The thesis began with the primary questions: "Is there a framework for applying law when considering the employment of computer network attack?" and if so, "Is the framework applied consistently throughout the Department of Defense?" Research, summarized in the opening paragraph above, shows there are the beginnings for a framework; however, it is not complete and is not applied consistently throughout the Department of Defense. This concluding chapter illuminates the key points of the research. First, computer network attack is shown to meet the necessary criteria for analysis by the laws of armed conflict. Next, four general principles of the laws of armed conflict, military necessity, unnecessary suffering, proportionality, and discrimination are

used as benchmarks to characterize the existing Schmitt framework of analysis. This framework is only sufficient for determining whether computer network attack surpasses the United Nations Article 2 (4) threshold for force. The third phase of research interviewed information operators and their lawyers. These interviews revealed the existence of the Schmitt framework but, showed the framework was not applied consistently throughout the information operations community. The final phase of research shows how complex organizational structures, unclear chains of command, and lack of coordinated legal counsel across commands, challenges any consistent application of the laws of armed conflict to computer network attack within the Department of Defense.

Why Is a Framework Necessary?

Conclusion 1. The United States military must consider the laws of armed conflict when employing computer network attack in combat. This statement assumes the United States military has entered into a conflict where the use of force has gone beyond the threshold set by the United Nations Charter, Article 2 (4). The argument is based on evidence showing computer network attack meets the definition of a weapon, produces effects similar to conventional weapons, and that commanders have a responsibility to consider its effects.

Computer network attack meets the definitions of "means," "weapon," and "armed" using the dictionary as the a-priori source. These words link computer network attack to the laws of armed conflict. Next, the Geneva Protocol I of 1977 states, "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under obligation to determine whether its employment would,

in some or all circumstances, be prohibited by the Protocol or by any other rule of international law applicable to the High Contracting Party" (Protocol Additional to the Geneva Conventions 1977, Part 3, Section I, Article 36). Based on this requirement, the United States military must determine the legality of computer network attack's effects.

The effects of computer network attack are potentially no less destructive than those produced by more physical means. An attacker, modifying lines of computer code, can today achieve the same effects as a fighter pilot dropping a munition on a target. Brigadier General David A. Deptula captured this type of warfare when he speaks of "control" as, "the idea that an enemy organization's ability to operate as desired is ultimately more important than the destruction of the forces it relies on for defense" (Deptula 2001, 11). What then are the responsibilities of command placed on commanders empowered to use computer network attack?

The concept of "lawful orders" requires leaders to understand the means and consequences of computer network attack with respect to the laws of armed conflict and train their subordinates to have those same understandings. Commanders and their subordinates must also clearly understand the chain of command and the authority vested in the leaders at each level of that chain. This authority is based on the military customs of commissioning officers, appointing those officers to command, and the subsequent organization and manning of positions within organizations.

A Framework of Analysis for Computer Network Attack?

Conclusion 2**.** <u>A basic framework of analysis for applying the laws of armed conflict to computer network attack exists in the form of the Schmitt Analaysis</u>. Author Thomas Wingfield in his book, *The Law of Information Conflict; National Security Law*

in Cyberspace, reveals a framework of analysis for computer network attack by Naval War College instructor Michael Schmitt. The tool uses the criteria of severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy to measure whether the level of force of computer network attack crosses the threshold into combat as defined by Article 2 (4) of the United Nations Charter.

Conclusion 3. The Schmitt analysis only determines the transition of computer network attack from *jus ad bello* to *jus in bello* but does not answer what portions of the laws of armed conflict apply to *jus in bello*. The analysis tool measures the level of each of the six criteria listed above and determines whether computer network attack is directed against the "territorial integrity or political independence" of another nation and whether the force resembles characteristics of more conventional means of military force. The framework helps determine whether the act is part of events below or leading up to the level of warfare or part of combat operations. While the analysis tool can indicate computer network attack's use as a force in combat, the framework does not say whether the use of such force is permissible in combat. The Schmitt analysis lacks the ability to link the force to the law of armed conflict's principles of military necessity, unnecessary suffering, proportionality, and discrimination.

Current State of Affairs

Conclusion 4**.** The Schmitt Analysis is rarely used within the Department of Defense information operations community. The Schmitt analysis was automated by Richard Moore, a contractor working for the Air Intelligence Agency, and the Joint Chiefs of Staff are incorporating the program into an upcoming version of its Joint Operation Planning and Execution System software. The only current use of the

framework is by the Information Operations Planners Course at the Air Force's Special Operations School at Hurlburt Air Force Base, Florida. These are the only two considerations of the Schmitt analysis by the Department of Defense uncovered in this thesis.

Conclusion 5. Lack of a clear organizational structure for information operations leads to potential inconsistencies in the application of law to computer network attack. Legal counsel is assigned to each Department of Defense organization assigned a computer network attack role. An unclear structure for information operations organizations is therefore indicative of a sub-optimal legal structure supporting this means of force. Lawyers interviewed revealed that legal advice is made on a case-by-case basis for computer network attack and that no formal process exists for codifying such legal debate. Also, separate structures for offense and defense result in legal teams associated with each but no experience base in both disciplines. Annual information operations conferences are held by the Department of Defense General Counsel, by the Air Force Staff Judge Advocate School, and by the Judge Advocate General's School of the Army, but there is no actionable output as a result of these forums.

Conclusion 6. Training for lawyers and by lawyers assigned to the information operations community is inadequate for a coherent and consistent application of the laws of armed conflict to computer network attack. Research showed that, at the extremes, lawyers are trained in both technology and how law applies to that technology whereas some lawyers receive no training at all and make no special effort to tailor the laws of armed conflict to computer network attack. The Aerospace Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance Agency's

course for information operations lawyers is the only such course in the Department of Defense. Similarly, the Information Operations Planner Course at Hurlburt Air Force Base, Florida is the only formal course covering the laws of armed conflict as applied to computer network attack. Finally, the Joint Task Force Computer Network Operations receives tailored law of armed conflict training for its information operators while the Air Force's 67th Information Operations Wing legal staff gives only the standard law of armed conflict briefing available to all members of the uniformed services.

Challenges

A New Framework

Recommendation 1. The Department of Defense should adopt the Schmitt Analysis as its standard framework for analyzing computer network attack with respect to the laws of armed conflict as a means of force. Although this framework only addresses computer network attack's level of force, it remains a useful first step in deciding if that force is part of combat operations. It is also the only framework in existence to address this issue. Incorporation into the Joint Chiefs of Staff's planning software should send a signal to the legal community that its structure and use should be taught to all information operators at all levels of the Department of Defense.

Recommendation 2. The Department of Defense General Counsel should build a more comprehensive framework of analysis for applying the laws of armed conflict to computer network attack based on the Schmitt analysis. Adoption of the Schmitt analysis by the Department of Defense's joint community lays the foundation for a more complete framework. Such a framework should examine the criteria for legal application of computer network attack in combat by addressing the principles of military necessity,

unnecessary suffering, proportionality, and discrimination. Thomas Wingfield's research is the most thorough to date and his law of armed conflict analogies tie computer network attack to more conventional methods of attack. The Office of the General Counsel should establish criteria from Wingfield's work and link them to the criteria in the Schmitt analysis.

Information Warfare Organization

Recommendation 3. Armed services should construct functionally organized information warfare structures and chains of command. Functional organizations capitalize on the principles of unity of command, mass, and economy of force. One commander, with the authority to conduct computer network attack and a clearly organized chain of command, allows the efficient massing of force. That commander can establish priorities for funding and training to ensure computer network attack achieves its combat potential. A single commander can also determine objectives and place the preponderance of force against those targets and not waste them on secondary objectives.

Recommendation 4. The Department of Defense and its branches of the armed services should continue to consolidate offensive and defensive capabilities for information operations. The potential speed of a computer network attack against our nation requires an offensive computer network attack capability with equal quickness. The technologies of computer network defense and attack are often the same and therefore lessons learned in one discipline are readily transferable to the other for both the information operations and legal communities. Joint doctrine recognizes the synergies of joining computer network defense and attack and the creation of the Joint Task Force Computer Network Operations is a manifestation of this doctrine. The individual

services should consolidate stove-piped structures for offense and defense to achieve the same synergies.

The Lawyer/Operator Relationship

Recommendation 5. Lawyers assigned to information operations organizations should receive information technology training. The Department of Defense should create a program for lawyers assigned to information operations organizations similar to the Medical Law Consultant Program that exposes medical lawyers to the practice of medicine. The Joint Task Force Computer Network Operations' training program should serve as a benchmark for the creation of such a program.

Recommendation 6. The Department of Defense General Counsel should establish a tailored program for teaching the laws of armed conflict as applied to the information operations. This tailored program should include the Schmitt analysis and incorporate Wingfield's analogies relating the principles of military necessity, unnecessary suffering, proportionality, and discrimination to computer network attack. This program should consist of training for both lawyers and information operators. The Air Force's Special Operations Command's Information Operations Planners Course and Aerospace Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance Agency's course for information operations lawyers offer potential sources for starting such a training program.

Recommendations for Further Study

Developing a more complete framework of analysis for computer network attack based on the Schmitt analysis is the primary area for further study. This research must receive support from both the legal and information operations communities to ensure

feasibility, acceptability, and suitability. Once developed, the Department of Defense should apply this framework to other information operations disciplines to provide for continuity. This continuity is necessary for a coherent and codified framework accepted and used by the United States military. Other areas for research include examining the value of a single commander with a functional command structure to employ information operations and an organizational theory study showing the optimal processes and structures for the information operations community and its legal staffs.

Closing Thoughts

United States national security strategy, military strategy, service doctrine and experts in the field of security studies agree information operations and computer network attack will be featured more often in the use of military force. The introduction of new means of force throughout history were examined in the context of social norms. Computer network attack is no exception. United States Air Force Major Karl Kuschner said it best when he wrote in *Airpower Journal*, "The greatest responsibility that lies on the shoulders of the armed forces will not allow its leaders to walk blindly down the information armory, choosing and employing new weapons without regard to consequences" (Kuschner 2002, 7). Key to fulfilling that responsibility is adopting the Schmitt framework of analysis for computer network attack, modifying that framework with respect to the laws of armed conflict's four general principles, and providing the necessary force structure and training to execute such a framework. Only under these conditions will computer network attack reach its combat potential in the ethical conduct of warfare.

APPENDIX A

Interview Questions

1. Do the laws of armed conflict apply to computer network attack?

   Follow-on: Why?

2. Is distinguishing "means" from the "effects" of computer network attack useful?

   Follow-on: Why?

3. Which is more important to the application of the laws of armed conflict to computer network attack…means or effects?

   Follow-on: Why?

4. Is there an existing legal framework for applying laws of armed conflict to computer network attack?

   Follow-on: If so what does it consist of?

5. What processes or policies are used for applying the laws of armed conflict to computer network attack?

   Follow-on: Are they applied consistently?

6. What efforts do you make to ensure consistent application of the law to computer network attack throughout the Department of Defense or your service?

7. What is the role of legal counsel in the application of computer network attack?

8. Do you have a good working relationship with (legal counsel / information operators)?

   Follow-on: Describe that relationship.

9. Are you trained on or do you train the laws of armed conflict as they relate to computer network attack?

   Follow-on: If so describe that training.

10. Do you cross-flow training standards, policies, briefings with your peers in other information operation organizations?

    Follow-on: If so, to whom?

APPENDIX B

Individuals Interviewed

Blake, Colby. Office of the Staff Judge Advocate, Air Intelligence Agency, Lackland Air Force Base, Texas. (210) 977-4525

Bordera, Michael, Captain, United States Air Force. 67th Information Operations Wing Legal Office, Lackland Air Force Base, Texas. (210) 977-2291.

Dhillon, Joseph, Lieutenant Colonel, United States Air Force. Office of the Staff Judge Advocate, United States Space Command, Peterson Air Force Base, Colorado. (719) 554-9193

Hanscom, Shannon, Major, United States Air Force. 67th Information Operations Wing Legal Office, Lackland Air Force Base, Texas. (210) 977-2291.

Laedlein, Charles, Colonel, United States Air Force (Retired). Chief Legal Counsel, Air Force Communications Agency, Scott Air Force Base, Illinois. (618) 229-6060.

Merz, Alexander, Captain, United States Air Force. Instructor, Information Operations Planner Course, Air Force Special Operations Command, Hurlburt Air Force Base, Florida. DSN: 579-1884.

Moore, Richard. Contractor, Joint Information Operations Center, Lackland Air Force Base, Texas. (210) 977-4658

Moore, Tyler, Captain, United States Air Force. Instructor, Information Operations Planner Course, Air Force Special Operations Command, Hurlburt Air Force Base, Florida. DSN: 579-1884.

Williamson, Charles, Lieutenant Colonel, United States Air Force. Chief Legal Counsel, Joint Task Force Computer Network Operations, United States Space Command, Arlington, Virginia. (703) 607-6327.

Wingfield, Thomas. Aegis Research Corporation, Falls Church, Virginia. (703) 610-9293.

APPENDIX C

Interviews

The following interviews were conducted by telephone from Ft. Leavenworth, Kansas. Interviews were conducted using the question outline in Annex A with the exception of the Wingfield interview, which was used to verify information in his book and in this thesis. The interviews are identified by alphabetic letter to provide the interviewee non-attribution and academic freedom of speech. Where individuals are quoted in the text of the thesis, their permission was granted, and those quotes do not appear in the interview notes.

APPENDIX C

Interview A

Q1. Yes. The military publicly acknowledges computer network defense and computer network attack.as capabilities and has designated units for those capabilities. A unit employing computer network attack must consider the laws of armed conflict just as an F-16 squadron must consider those laws.

Q2. Yes. Each has specific utility in applying the law. The effects of computer network attack are most recognizable as being addressed in the laws of armed conflict. Certainly the use of computer network attack to achieve the same outcome as a bomb or other explosive is evidence of this. The means also have an impact. We need to be cognizant of the infrastructure we use to conduct any attack. If that infrastructure is primarily civilian built and controlled than are we making that infrastructure subject to attack? These are the types of issues the legal field is struggling with right now.

Q3. I don't think you can put a greater value on either, although the laws of armed conflict will chiefly be concerned with effects.

Q4. (Interviewee was specifically asked about the Wingfield text and the Schmitt analysis.) Yes, I'm aware of Mr. Wingfield's book. I know the Information Operations Planner Course offered by the Special Operations Command has portions of the Schmitt analysis in their briefing slides. As I said before, however, these cases [of computer network attack] are reviewed on a case by case basis. We would certainly use the laws of armed conflict as a baseline for our analysis but there is no standard cookbook method and really shouldn't be….every case will be different.

Q5. Like I said this is done on a case by case basis. Is there room for improvement in the areas of training lawyers on this topic…absolutely. More comprehensive training will lead to better consistency.

Q6. Right now the only efforts I'm aware of are the annual information operations conference held at the JAG school at Maxwell Air Force Base.

Q7. We are advisors. It is no different than any other relationship where lawyers are advising commanders on the conduct of warfare.

Q8. I would say the relationship is a good one though no commander likes to be told no. This is such a new area and both sides are on new ground so I think commanders are more likely to actively engage with the legal side of the house.

Q9. Yes. I've received training on the laws of armed conflict many times but currently we do not specifically train the laws of armed conflict as they apply to computer network attack.

Q10. No. Well yes if you consider the conferences on information operations. No, there are no formal products that I can think of as a result of those conferences.

APPENDIX C

Interview B

Q1. Yes. Computer network attack should be considered a means of force like any other means of force used by the military

Q2. Yes. Well. . . considering the previous question, [effects] are really the prime consideration where the laws of armed conflict are concerned. Those laws were designed to control conduct of combatants in terms of their effects on noncombatants.

Q3. I would have to say effects. Like I said previously this is what the law addresses.

Q4. No, not that I am aware of. Yes I've heard of [Wingfield's book.] One of the lawyers we use during training incorporates his work in his slide presentation.

Q5. We do have a legal staff that provides input on a case-by-case basis and we do use lawyers as part of our training. As for consistency across the Air Force or Department of Defense I would say the same case-by-case practices exist.

Q6. Nothing.

Q7. They provide guidance but ultimately the decision rests with the commander.

Q8. (Laughter) Yeah, I know where you are going with this one but I'd have to say the relationship is pretty good. We respect their advice though we are not always in agreement. I do think its important that the legal team plays a part in our mission.

Q9. Yes on both counts. We emphasize the role of the legal team in planning information operations.

Q10. No.

APPENDIX C

Interview C

Q1. Yes. Technology is now capable of creating destructive effects. Just think of the damage some of the recent computer viruses have done to our [Air Force] networks. The "I Love You" virus caused damage to our e-mail servers thereby shutting down communications. If you shut down network and telephone communications, using CNA, of a hospital or for the general public during conflict you start to enter into the realm of noncombatants. This is exactly what the laws of armed conflict address.

Q2. Yes. The means are more readily addressed through domestic laws both U.S. and international whereas the effects or outcomes are treated by international law such as the laws of armed conflict. Just applying our domestic laws to CNA's means is a challenge before we even consider its effects.

Q3. I think they are both important. You can't discard one or the other though if you are just examining the laws of armed conflict you probably want to focus on effects.

Q4. No. We really don't have a good grip on how to apply the law in this area and it is ripe for study.

Q5. Everyone has their own approach. Everyone is doing their own thing within the bounds of their professional training. There is no organized way or process for applying the law to CNA.

Q6. The best we have to offer right now is an annual conference at the JAG school down at Maxwell [Air Force Base.] I would not call this an effort to standardize training as much as it is an opportunity to expose areas for further study and to make lawyers aware of new rulings and decisions where technology is concerned.

Q7. We have to ensure information operators are advised of the consequences of their actions. Because this CNA is so new and the communities are so few, sometimes the lawyers who are thinking about this the most don't have direct impact on these people. We have to ensure our voice is heard and that operators don't dismiss our advice just because the technologies are commonly used in our high-tech world.

Q8. Yes, I think so but, it isn't always as smooth as it should be. We suffer from the "lawyer stigma" and that is why its important we keep making the effort to ensure our voice is heard.

Q9. No. This would be a great subject for someone to develop training specifically for computer network attack.

Q10. Yes. We pass items along to others we think might find them useful but, there is no formal process that requires this.

APPENDIX C

Interview D

Q1. Yes, but, I only provide the standard law of armed conflict briefing to all wing members. The information operations squadrons have their own legal counsel who provides specific guidance.

At this point the individual felt the legal counsel for the information operations squadron was more qualified to answer the remaining questions and referred the author to this source.

APPENDIX C

Interview E

Q1. Yes. We've included computer network attack as part of our arsenal of weapons and therefore it is subject to the rules just like any other weapon.

Q2. I suppose so. If you think of it though, the laws of armed conflict are pretty much concerned with the effects and don't care much about the means

Q3. Like I said, the effects are more important to the laws of armed conflict.

Q4. Have you checked out Thomas Wingfield's book, *The Laws of Information Conflict*? He uses the Schmitt Analysis as a framework for applying law to computer network attack. This is the only framework I'm aware of and it is being incorporated by the Joint Staff in its planning efforts.

Q5. I think we're making progress but I can't say that Wingfield's framework is the one and only standard. I think you'll find the lawyers will tell you that the process for giving advice is the same as any other discipline of attack and targeting. Legal advice is given based on the situation at hand. Hopefully the incorporation of the Schmitt Analysis into Joint Planning will at least help standardize consideration for employment of computer network attack in the planning stages.

Q6. I developed the software for that the Joint Staff is adopting. At the end of the day it's not up to me to standardize. The policy makers must make those decisions.

Q7. As I said before, they offer guidance as they would in any other attack discipline.

Q8. I think its fair to say that the same tension exists as in any other lawyer client relationship in the military. The operator will always feel like he's being held back but, you can't ignore the role of the legal side of the house in the business of conducting an attack.

Q9. I've never been specifically trained but I was a reviewer for Wingfield's book.

Q10. Only the effort of developing the software and having the Joint Staff adopt it for use.

APPENDIX C

Interview F

Q1. Yes. The potential effects of using computer network attack are not much different in some cases than that of more conventional uses of force.

Q2. I think the law addresses both. The laws of armed conflict address both but, I think the effects are less contentiously debated than the means. What I mean is that there exists an argument over whether computer network attack is "armed force." There is little disagreement though, that the effects of computer network attack can be measured on the same scale as our conventional means of attack.

Q3. I think we pretty much covered that in the last question

Q4. No.

Q5. I'm not sure you can say the laws of armed conflict are specifically addressed each and every time but, we apply law to computer network attack on an "eaches" basis . . . that is every case is different and deserves individual attention. I suppose that leaves room for inconsistencies as it does in any other application of the law.

Q6. Nothing specifically. There are several conferences each year which address the subject but no tangible results in standardization are produced. It is more an issue of awareness of new issues. The two conferences I can think of are at Fort Meade and Maxwell Air Force Base.

Q7. We are advisors. The operators and specifically the commanders must make judgements based on that advice.

Q8. I think it is getting better but there is always going to be a hesitancy on the part of operators to accept lawyers as part of the team when the lawyer is sometimes the only voice of dissent.

Q9. I have been trained and have trained the laws of armed conflict during my military career but that training was never specifically geared toward computer network attack.

Q10. No. There are no overt efforts to do this other than the conferences I mentioned earlier.

APPENDIX C

Interview G

Q1. Yes. That is one of the areas we look at. As a form of attack, we must consider these laws. The outcome of an F-16's attack on a target and a computer's ability to generate the same effect, in certain circumstances, is closing every day.

Q2. Yes. Effects are the real area of concern although the means come into play when you talk about using different pieces of the enabling infrastructure.

Q3. Well as I just said, the effects are the area of concern when looking at the laws of armed conflict. People mistake the symptom for the cause when it comes to new weapons. It is not the weapon people are ultimately concerned with but the effect that weapon has.

Q4. No. Yes I have heard of Thomas Wingfield's work but, as far as I know there is no effort to make his or any other analysis a standard throughout the Department of Defense.

Q5. The DoD's General Counsel provided some guidance in the form of an assessment of international legal issues in information operations but that assessment does not contain a specific framework for applying law. The structure for applying law is the same for computer network attack as it is for other areas in the military. Each organization has its own legal staff that provides tailored advice.

Q6. We certainly share information within the Major Command and when we attended conferences addressing information operations. I can't say we make a concerted effort throughout the Air Force to ensure consistent application of the law. Again though, law is left to interpretation in the early stages of any new capability like computer network attack.

Q7. We are counselors and advisors. At the end of the day we cannot be the decision makers. Leaders and commanders must make those decisions based on sound advice.

Q8. Yes. We immerse ourselves in the operations community. I even have two offices one on the legal side and one on the operations side. That doesn't mean we see eye-to-eye on every issue but the relationship is strong.

Q9. I've received law of armed conflict training but I do not train operators on the subject directly. They are discussed as we go through scenarios.

Q10. I think I covered that earlier when we talked about the conferences.

APPENDIX C

Interview H

Q1. Yes. Attack is attack. If you are on the receiving end you don't really care how it happened if you're suffering.

Q2. I'm not sure there is a great need to do so. I would say that the effects are what we are most interested in.

Q3. Like I said, effects.

Q4. No. I don't think so. None that I can think of.

Q5. We receive advice from the local legal staff and from visiting lawyers. I really can't comment on how others get their legal advice.

Q6. None.

Q7. They give advice, we listen and debate the issue, and a position is presented to the commander. The commander normally meets with the senior staff and his lawyer before any decision is made.

Q8. Yes but, I have to admit we don't view them the same way we do the other operators. They are like a profession within a profession if you know what I mean. I think they definitely have a role but we need to be the one's that take action.

Q9. Yes. I have received law of armed conflict training. It's up to us though to make the connection to information operations.

Q10. No.

APPENDIX C

Interview I

Q1. Yes. Computer network attack is similar to other forms of attack in that it produces similar effects. A bomb and computer attack can now achieve some of the same things.

Q2. Yes. They need to be considered separately. Currently there is a huge debate in the legal community on whether the analysis of computer network attack should be effects-based or means-based. I think there has to be an analysis that considers both.

Q3. The laws of armed conflict primarily focus on effects and we assume that computer network attack is capable of generating effects similar to an F-16 when we do any analysis.

Q4. No. This is part of the problem. We normally cover the basic principles of military necessity, unnecessary human suffering, discrimination, and proportionality when we do any analysis but there is no standard guide.

Q5. It's so varied. I can't say with any certainty that what we do here is the same as other legal offices supporting information operators in other services.

Q6. We attend conferences. I attended the last information operations conference at the JAG school at Maxwell [AFB]. You are right that these conferences are informational and do not produce any tangible output for standardization.

Q7. We are advisors. Commanders can always choose to ignore our advice in which case we document our stance but, in the end that is why the commander retains accountability.

Q8. Yes. I think this is due to the fact that the information operations community was closely tied to the intelligence community. The intelligence community was regulated by intelligence oversight rules and so information operators are used to having lawyers as part of the operational environment. They still don't like it when we say no but that is part of the role of lawyers I discussed earlier.

Q9. Only at the conferences but, no specific or formal training.

Q10. Again only at the conferences and only information awareness.

APPENDIX C

Interview J

The following interview was conducted with Thomas Wingfield, the author of *The Law of Information Conflict, National Security Law in Cyberspace*.

Q1. Do you know whether anyone in addition to the Joint Staff has adopted your work within the Department of Defense?

A1. I am aware of the organizations you mentioned such as the Information Operations Planners' Course at Hurlburt but on the whole I would say only ten to twenty percent of DoD information operations organizations may be using my work.

Q2. Would you agree there is no organized effort to ensure the laws of armed conflict are applied consistently throughout the Department of Defense to computer network attack?

A2. Yes. That is a fairly accurate statement.

Q3. You're use of the Schmitt Analysis is useful for determining the level of force of computer network attack. Is there anything that directly relates the effects of that force to the four general principles of the laws of armed conflict you mention in your book?

A3. No. No additional piece of the framework that is. Others have covered this issue in an academic context but, there is no work that I am aware of on the practical side.

Q4. Would you agree the Department of Defense should make an effort to standardize the application of the laws of armed conflict to computer network attack?

A4. Yes, but, I would caution that each case of computer network attack is different and any effort at standardization needs to accommodate those differences. The framework needs to be a guide and not a restraint.

WORKS CITED

Ackerman, Robert K. March 2002. *"Technology Empowers Information Operations in Afghanistan*." Signal: 17-20.

Air Combat Command Public Affairs. 26 October 2000. "Air Intelligence Agency merges with Air Command Combat." *ACC Combat Command News Service*, [Online] Available http://www2.acc.af.mil/accnews/Oct00/000343.html.

Air Force Information Warfare Center. 15 March 2002. *"Air Force Information Warfare Center Organizational Chart*." [Online] Available http://afiwcweb.lackland.af.mil/.

Aldrich, Richard W. 1996. *The International Legal Implications of Information Warfare*. Colorado Springs: United States Air Force Institute for National Security Studies.

Arquilla, John, and David Ronfeldt. 1996. *The Advent of Netwar*. Santa Monica, California: RAND.

Barnett, Jeffery R. 1996. *Future War; An Assessment of Aerospace Campaigns in 2010*. Maxwell Air Force Base, Alabama: Air University Press.

Barney, Steven M. 2001. "Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace." *Chairman of the Joint Chiefs of Staff Essay Competition*: 1-22.

Bass, Carla D. 1999. "Building Castles on Sand: Underestimating the Tide of Information Operations." *Airpower Journal* 13, no. 2: 27-45.

Best, Geoffrey. 1980. *Humanity in Warfare*. New York: Columbia University Press.

Biddle, Tami Davis. 1994. "Air Power." in *The Laws of War: Constraints on Warfare in the Western World*. Michael Howard, George J. Andreopoulos, and Mark R. Shulman, eds. New Haven, Connecticut: Yale University Press.

Buchan, Glenn. March 1996. "Information War and the Air Force: Wave of the Future? Current Fad?" *RAND Project Air Force Issue Paper*, [Online] Available http://www.rand.org/publications/IP/IP149.

Chairman, Joint Chiefs of Staff. 1999. *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations.* 4th ed. Washington, D.C.: United States Government Printing Office, August.

_____. 1994. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.* Washington, D.C.: United States Government Printing Office.

_____. 1998. Joint Publication 3-13, *Joint Doctrine for Information Operations.* Washington, D.C.: United States Government Printing Office.

_____. 2000. *Joint Vision 2020*. Washington, D.C.: United States Government Printing Office.

_____. 25 March 2002. Joint Chiefs of Staff Instruction 5810.01B, *DoD Law of War Program*. Washington, D.C.: United States Government Printing Office.

Charter of the United Nations. 1945. in *Basic American Documents.* eds. George B. Huszar, Henry W. Littlefield, and Arthur W. Littlefield, 290-335. Ames, Iowa: Littlefield, Adams, and Company, 1953.

Convention (IV) Respecting the Laws and Customs of War on Land. 1907. in *Documents on the Laws of War*. eds. Adam Roberts and Richard Guelff, 44-59. Oxford: Clarendon Press, 1982.

Cordesman, Anthony H. 2002. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, Connecticut: Praeger.

Defense Information Systems Agency. 14 June 2000. "Fact Sheet: Global Network Operations and Security Center (GNOSC) Command Center." [Online] Available http:www.disa.mil/info/fsgnosc.html.

Denning, Dorothy E. 1999. *Information Warfare and Security.* Reading, Massachusetts: Addison-Wesley.

Department of the Air Force, Headquarters Air Intelligence Agency. 1 May 1998. *"Air Intelligence Agency Mission Directive 1502: Air Force Information Warfare Center*." [Online] Available http://pdo.pdc.aia.af.mil/library/pubs.

Department of the Army. 2001. U.S. Army Field Manual 3-0, *Operations*. Washington, D.C.: United States Government Printing Office.

_____. 1956. U.S. Army Field Manual 27-10, *The Law of Land Warfare*. Washington, D.C.: United States Government Printing Office.

_____. 1997. U.S. Army Field Manual 101-5-1, *Operational Terms and Graphics*. Washington, D.C.: United States Government Printing Office.

Deptula, David A. 2001. *Effects-Based Operations: Change in the Nature of Warfare*. Arlington, Virginia: Aerospace Education Foundation.

Dhillon, Joseph, Lieutenant Colonel, United States Air Force. 19 March 2002. Office of the Staff Judge Advocate, United States Space Command, Peterson Air Force Base, Colorado. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas.

DiCenso, David J. 1999. "IW Cyberlaw: The Legal Issues of Information Warfare." *Airpower Journal* 13, no. 2: 85-102.

Goldfein, David L. 2001. *Sharing Success, Owning Failure: Preparing to Command in the Twenty-First Century Air Force*. Maxwell Air Force Base, Alabama: Air University Press.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. 1997. *Information Warfare and International Law*. Washington, D.C.: National Defense University Press.

Headquarters Air Force Doctrine Center. 1997. Air Force Doctrine Document 1, *Air Force Basic Doctrine*. Washington, D.C.: United States Government Printing Office.

_____. 2000. Air Force Doctrine Document 2, *Organization and Employment of Aerospace Power*. Washington, D.C.: United States Government Printing Office.

_____. 1998. Air Force Doctrine Document 2-5, *Information Operations*. Washington, D.C.: United States Government Printing Office.

Huszar, George B., Henry W. Littlefield, and Arthur W. Littlefield, eds. 1953. *Basic American Documents.* Ames, Iowa: Littlefield, Adams, and Company.

Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. 1997. *Grand Strategy for Information Age National Security; Information Assurance for the Twenty-first Century*. Maxwell Air Force Base, Alabama: Air University Press.

Kuschner, Karl. 15 March 2002. "Legal and Practical Constraints on Information Warfare." *Airpower Journal*, [Online] Available http://www.airpower.au.af.mil/airchronicles/cc/kuschner.html.

Laedlein, Charles, Colonel, United States Air Force (Retired). 5 March 2002. Chief Legal Counsel, Air Force Communications Agency, Scott Air Force Base, Illinois. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas.

Libicki, Martin C. 1995. *What is Information Warfare*? Washington, D.C.: National Defense University Press.

Manual for Courts-Martial (2000 Edition). 2000. Washington, D.C.: United States Government Printing Office.

Moore, Richard. 22 April 2002. Contractor, Joint Information Operations Center, Lackland Air Force Base, Texas. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas.

Moore, Tyler, Captain, United States Air Force. 22 April 2002. Instructor, Information Operations Planner Course, Air Force Special Operations Command, Hurlburt Air Force Base, Florida. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas.

Morris, William, ed. 1973. *The American Heritage Dictionary of the English Language*. Boston: Houghton Mifflin Company.

Nabulsi, Karma. 7 May 2002. "Jus ad Bellum/Jus in Bello." [Online] Available http://www.crimesof war.org/thebook/jus-ad-bellum.html.

Peterson, John L. 1996. "Information Warfare: The Future." in *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds. Fairfax, Virginia: Armed Forces Communications and Electronics Association Press.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). 1977. in *Documents on the Laws of War*. eds. Adam Roberts and Richard Guelff, 389-446. Oxford: Clarendon Press, 1982.

Roberts, Adam, and Richard Guelff, eds. 1982. *Documents on the Laws of War*. Oxford: Clarendon Press.

Schwartau, Winn. 1996. "Ethical Conundra of Information Warfare." in *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds. Fairfax, Virginia: Armed Forces Communications and Electronics Association Press.

Secretary of Defense. 2001. *Quadrennial Defense Review Report*. Washington, D.C.: United States Government Printing Office.

Seffers, George I. 09 May 2001. "DOD Braced for Cyberattack." *Federal Computer Week*, [Online] Available http://www.fcw.com/fcw/articles/2001/0507/web-hack-05-09-01.asp.

Strassman, Paul A. 1995. *The Politics of Information Management: Policy Guidelines*. New Canaan, Connecticut: The Information Economics Press.

Tangredi, Sam J. 2001. "The Future Security Environment, 2001-2025: Toward a Consensus View." in *QDR 2001; Strategy-driven Choices for America's Security.* Michele A. Flourney, ed. Washington, D.C.: National Defense University Press.

The Associated Press. 19 November 2001. "Air Force officials say disputes in central command hampering U.S. action." [Online] Available http://www.accessatlanta.com/ajc/terrorism/military/afghan/1119disputes.html.

The White House. 2000. *A National Security Strategy for a Global Age*. Washington, D.C.: United States Government Printing Office.

Toffler, Alvin and Heidi. 1993. *War and Anti-war; Survival at the Dawn of the 21st Century*. Boston: Little, Brown and Company.

United States Congress. House. 17 May 2001. House Armed Services Committee, Military Readiness Subcommittee. *Hearing on Information Technology: Examining Vulnerabilities of Department of Defense Networks.* [Online] Available http://www.iwar.org.uk/cip/resources/ia-hearing-2001-05/.

United States Army Command and General Staff College. 2001. Student Text 20-10, *Master of Military Art and Science (MMAS) Research and Thesis*. Fort Leavenworth, Kansas: United States Army Command and General Staff College.

United States Army Command and General Staff College. 2001. Student Text 27-1, *Military Law*. Fort Leavenworth, Kansas: United States Army Command and General Staff College.

United States Space Command. 14 December 2001. "*JTF-CNO Fact Sheet*." [Online] Available http:www.spacecom.af.mil/usspacecom/jtf-cno.htm.

United States Transportation Command, JOPES Training Organization. 2000. *JOPES Basic Operations Course Training Manual.* Scott Air Force Base, Illinois: United States Transportation Command.

University of Texas at Austin Graduate School of Library and Information Science. 9 October 2001. "Discourse Analysis." [Online] Available http://fiat.gslis.utexas.edu/~palmquis/courses/discourse.htm.

Waltz, Edward. 1998. *Information Warfare: Principles and Operations*. Boston: Artech House.

Williamson, Charles, Lieutenant Colonel, United States Air Force. 19 March 2002. Chief Legal Counsel, Joint Task Force Computer Network Operations, United States Space Command, Arlington, Virginia. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas.

Wingfield, Thomas C. 2000. *The Law of Information Conflict: National Security Law in Cyberspace*. Falls Church, Virginia: Aegis Research Corporation.

_____. 29 April 2002. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas.

BIBLIOGRAPHY

Books

Aldrich, Richard W. *The International Legal Implications of Information Warfare*. Colorado Springs: United States Air Force Institute for National Security Studies, 1996.

Arquilla, John, and David Ronfeldt. *The Advent of Netwar*. Santa Monica, California: RAND, 1996.

Barnett, Jeffery R. *Future War; An Assessment of Aerospace Campaigns in 2010*. Maxwell Air Force Base, Alabama: Air University Press, 1996.

Best, Geoffrey. *Humanity in Warfare*. New York: Columbia University Press, 1980.

Biddle, Tami Davis. 1994. "Air Power." in *The Laws of War: Constraints on Warfare in the Western World*. eds. Michael Howard, George J. Andreopoulos, and Mark R. Shulman, 140-159. New Haven, Connecticut: Yale University Press.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden, eds. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, Virginia: Armed Forces Communications and Electronics Association Press, 1996.

Cordesman, Anthony H. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, Connecticut: Praeger, 2002.

Denning, Dorothy E. *Information Warfare and Security.* Reading, Massachusetts: Addison-Wesley, 1999.

Goldfein, David L. *Sharing Success, Owning Failure: Preparing to Command in the Twenty-First Century Air Force*. Maxwell Air Force Base, Alabama: Air University Press, 2001.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. *Information Warfare and International Law*. Washington, D.C.: National Defense University Press, 1997.

Hildreth, Steven A. "Cyberwarfare." in *Cyberwarfare: Terror at a Click*, ed. John V. Blane, 4-23. Huntington, New York: Novinka Books, 2001.

Howard, Michael, George J. Andreopoulos, and Mark R. Shulman, eds. *The Laws of War: Constraints on Warfare in the Western World*. New Haven, Connecticut: Yale University Press, 1994.

Hubbuch, Susan M. *Writing Research Papers Across the Curriculum*, 4th ed. New York: Harcourt Brace College Publishers, 1996.

Huszar, George B., Henry W. Littlefield, and Arthur W. Littlefield, eds. *Basic American Documents.* Ames, Iowa: Littlefield, Adams, and Company, 1953.

Libicki, Martin C. *What is Information Warfare*? Washington, D.C.: National Defense University Press, 1995.

Negroponte, Nicholas. *Being Digital*. New York: Vintage Books, 1996.

Patton, Michael Quinn. *Qualitative Evaluation and Research Methods*, 2nd ed. London: Sage Publications, 1990.

Peterson, John L. 1996. "Information Warfare: The Future." in *Cyberwar: Security, Strategy, and Conflict in the Information Age*. eds. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 219-226. Fairfax, Virginia: Armed Forces Communications and Electronics Association Press.

Roberts, Adam, and Richard Guelff, eds. *Documents on the Laws of War*. Oxford: Clarendon Press, 1982.

Schwartau, Winn. 1996. "Ethical Conundra of Information Warfare." in *Cyberwar: Security, Strategy, and Conflict in the Information Age*. eds. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 243-250. Fairfax, Virginia: Armed Forces Communications and Electronics Association Press.

Strassman, Paul A. *The Politics of Information Management: Policy Guidelines*. New Canaan, Connecticut: The Information Economics Press, 1995.

Tangredi, Sam J. "The Future Security Environment, 2001-2025: Toward a Consensus View." in *QDR 2001; Strategy-driven Choices for America's Security.* Michele A. Flourney, ed. Washington, D.C.: National Defense University Press, 2001.

Toffler, Alvin and Heidi. *War and Anti-war; Survival at the Dawn of the 21st Century*. Boston: Little, Brown and Company, 1993.

Waltz, Edward. *Information Warfare: Principles and Operations*. Boston: Artech House, 1998.

Wingfield, Thomas C. *The Law of Information Conflict: National Security Law in Cyberspace*. Falls Church, Virginia: Aegis Research Corporation, 2000.

Periodicals and Articles

Ackerman, Robert K. *"Technology Empowers Information Operations in Afghanistan."* Signal, March 2002, 17-20.

_____. *"Army Cyberwarriors Prepare for Broader Future."* Signal, March 2002, 23-26.

Air Combat Command Public Affairs. "Air Intelligence Agency merges with Air Command Combat." *ACC Combat Command News Service*, [Online] Available http://www2.acc.af.mil/accnews/Oct00/000343.html, 26 October 2000.

Arquilla, John. "The Great Cyberwar of 2002." *Wired*, [Online] Available http://www.wired.com/wired/archive/6.02/cyberwar.html?topic=hacking_warez&topic_set=ne, February 1998.

Barney, Steven M. "Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace." *Chairman of the Joint Chiefs of Staff Essay Competition* (2001): 1-22.

Bass, Carla D. "Building Castles on Sand: Underestimating the Tide of Information Operations." *Airpower Journal* 13, no. 2 (Summer 1999): 27-45.

Dean, Joshua. "Defense Anti-Hacking Office Goes on the Offensive." *Government Executive Magazine*, [Online] Available http://www.govexec.com/dailyfed/0601/060501j1.htm, 5 June 2001.

DiCenso, David J. "IW Cyberlaw: The Legal Issues of Information Warfare." *Airpower Journal* 13, no. 2 (Summer 1999): 85-102.

Krebs, Brian. "Thirty Nations Sign Global Cybercrime Treaty." *Newsbytes*, [Online] Available http://www.infowar.com/law/01/law_112601c_j.shtml, 26 November 2001.

Kuschner, Karl. "Legal and Practical Constraints on Information Warfare." *Airpower Journal*, [Online] Available http://www.airpower.au.af.mil/airchronicles/cc/kuschner.html, 15 March 2002.

Meller, Paul. "European Union Set to Vote on Data Law." *The New York Times*, [Online] Available http://www.nytimes.com/2001/11/13/technology/13NET.html?todaysheadlines, 13 November 2001.

Nabulsi, Karma. "Jus ad Bellum/Jus in Bello." [Online] Available http://www.crimesofwar.org/thebook/jus-ad-bellum.html. 7 May 2002.

Olsen, Stefanie. "Time to Protect the Net from Terrorism?" *News.com*, [Online] Available http://www.zdnet.com/filters/printerfriendly/0,6061,5098497-2,00.html, 18 October 2001.

Seffers, George I. "DOD Braced for Cyberattack." *Federal Computer Week*, [Online] Available http://www.fcw.com/fcw/articles/2001/0507/web-hack-05-09-01.asp, 09 May 2001.

The Associated Press. "Air Force officials say disputes in central command hampering U.S. action." [Online] Available http://www.accessatlanta.com/ajc/terrorism/military/afghan/1119disputes.html, 19 November 2001.

Thomas, Timothy L. "Russian Views on Information-Based Warfare." *Airpower Journal* (Special Edition 1996): 25-35.

Tiboni, Frank. "DoD Deploys Cyber-Defense." *Defense News*, [Online] Available http://ebird.dtic.mil/Nov20011112cyber.htm, 12-18 November 2001.

University of Texas at Austin Graduate School of Library and Information Science. "Discourse Analysis." [Online] Available http://fiat.gslis.utexas.edu/~palmquis/courses/discourse.htm, 9 October 2001.

Verton, Daniel. "DOD Boosts IT Security Role." *Federal Computer Week*, [Online] Available http:www.fcw.com/fcw/articles/1999/FCW_100499_7.asp, 4 October 1999.

Government Documents

Chairman, Joint Chiefs of Staff. *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations*. 4th ed. Washington, D.C.: United States Government Printing Office, August 1999.

_____. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.* Washington, D.C.: United States Government Printing Office, 1994.

_____. Joint Publication 3-13, *Joint Doctrine for Information Operations.* Washington, D.C.: United States Government Printing Office, 1998.

_____. *Joint Vision 2020*. Washington, D.C.: United States Government Printing Office, 2000.

_____. Joint Chiefs of Staff Instruction 5810.01B, *DoD Law of War Program*. Washington, D.C.: United States Government Printing Office, 25 March 2002.

Council of Europe. *Convention on Cybercrime.* European Treaty Series no. 185. Budapest, 23 November 2001.

Department of the Air Force, Headquarters Air Intelligence Agency. *"Air Intelligence Agency Mission Directive 1502: Air Force Information Warfare Center*." [Online] Available http://pdo.pdc.aia.af.mil/library/pubs, 1 May 1998.

Department of the Army. U.S. Army Field Manual 3-0, *Operations*. Washington, D.C.: United States Government Printing Office, 2001.

_____. U.S. Army Field Manual 27-10, *The Law of Land Warfare*. Washington, D.C.: United States Government Printing Office, 1956.

_____. U.S. Army Field Manual 101-5-1, *Operational Terms and Graphics*. Washington, D.C.: United States Government Printing Office, 1997.

Headquarters Air Force Doctrine Center. Air Force Doctrine Document 1, *Air Force Basic Doctrine*. Washington, D.C.: United States Government Printing Office, 1997.

_____. Air Force Doctrine Document 2, *Organization and Employment of Aerospace Power*. Washington, D.C.: United States Government Printing Office, 2000.

_____. Air Force Doctrine Document 2-5, *Information Operations*. Washington, D.C.: United States Government Printing Office, 1998.

Manual for Courts-Martial (2000 Edition). Washington, D.C.: United States Government Printing Office, 2000.

Secretary of Defense. *Quadrennial Defense Review Report*. Washington, D.C.: United States Government Printing Office, 2001.

The White House. *A National Security Strategy for a Global Age*. Washington, D.C.: United States Government Printing Office, 2000.

United States Congress. House. House Armed Services Committee, Military Readiness Subcommittee. *Hearing on Information Technology: Examining Vulnerabilities of Department of Defense Networks.* [Online] Available http://www.iwar.org.uk/cip/resources/ia-hearing-2001-05/, 17 May 2001.

United States Army Command and General Staff College. Student Text 20-10, *Master of Military Art and Science (MMAS) Research and Thesis*. Fort Leavenworth, Kansas: United States Army Command and General Staff College, 2001.

United States Army Command and General Staff College. Student Text 27-1, *Military Law*. Fort Leavenworth, Kansas: United States Army Command and General Staff College, 2001.

United States Transportation Command, JOPES Training Organization. *JOPES Basic Operations Course Training Manual*. Scott Air Force Base, Illinois: United States Transportation Command, 2000.

Other Sources

Interviews

Blake, Colby. Office of the Staff Judge Advocate, Air Intelligence Agency, Lackland Air Force Base, Texas. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 19 March 2002.

Bordera, Michael, Captain, United States Air Force. 67th Information Operations Wing Legal Office, Lackland Air Force Base, Texas. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 22 April 2002.

Dhillon, Joseph, Lieutenant Colonel, United States Air Force. Office of the Staff Judge Advocate, United States Space Command, Peterson Air Force Base, Colorado. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 19 March 2002.

Hanscom, Shannon, Major, United States Air Force. 67th Information Operations Wing Legal Office, Lackland Air Force Base, Texas. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 22 April 2002.

Laedlein, Charles, Colonel, United States Air Force (Retired). Chief Legal Counsel, Air Force Communications Agency, Scott Air Force Base, Illinois. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 5 March 2002.

Merz, Alexander, Captain, United States Air Force. Instructor, Information Operations Planner Course, Air Force Special Operations Command, Hurlburt Air Force Base, Florida. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 19 March 2002.

Moore, Richard. Contractor, Joint Information Operations Center, Lackland Air Force Base, Texas. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 22 April 2002.

Moore, Tyler, Captain, United States Air Force. Instructor, Information Operations Planner Course, Air Force Special Operations Command, Hurlburt Air Force Base, Florida. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 22 April 2002.

Williamson, Charles, Lieutenant Colonel, United States Air Force. Chief Legal Counsel, Joint Task Force Computer Network Operations, United States Space Command, Arlington, Virginia. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 19 March 2002.

Wingfield, Thomas C. Aegis Research Corporation, Falls Church, Virginia. telephone interview by author, author's personal notes, Fort Leavenworth, Kansas, 29 April 2002.

Fact Sheets

Air Force Information Warfare Center. *"Air Force Information Warfare Center Organizational Chart*." [Online] Available http://afiwcweb.lackland.af.mil/, 15 March 2002.

Air Intelligence Agency. *"67 Information Operations Wing Units.*" [Online] Available http:www.aia.af.mil/homepages/67iow/units.cfm, 15 March 2002.

Defense Information Systems Agency. *"DISA Office of Regulatory/General Counsel."* [Online] Available http:www.disa.mil/main/gc/html, 28 November 2001.

_____. "Fact Sheet: Department of Defense Computer Emergency Response Team (DoD-CERT)." [Online] Available http://www.disa.mil/info/fs121999.html, 14 June 2000.

_____. "Fact Sheet: Global Network Operations and Security Center (GNOSC) Command Center." [Online] Available http:www.disa.mil/info/fsgnosc.html, 14 June 2000.

Department of the Air Force. "Air Intelligence Agency Fact Sheet." [Online] Available http:www.af.mil/news/factsheets/Air_Intelligence_Agency.html, 15 March 2002.

TNO Physics and Electronics Laboratory. "Information Warfare (IW) Links." [Online] Available http://www.tno.nl/instit/fel/intern/wkiwar5.html, 26 November 2001.

United States Space Command. "*JTF-CNO Fact Sheet*." [Online] Available http:www.spacecom.af.mil/usspacecom/jtf-cno.htm, 14 December 2001.

Papers

Black, Steven K. *This Page Under Construction: Information Warfare in the Post-Cold War World*. Pittsburgh: Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh Graduate School of Public and International Affairs, 1996. Ridgeway Viewpoints no. 96-1.

Buchan, Glenn. "Information War and the Air Force: Wave of the Future? Current Fad?" *RAND Project Air Force Issue Paper*, [Online] Available http://www.rand.org/publications/IP/IP149, March 1996.

Deptula, David A. *Effects-Based Operations: Change in the Nature of Warfare*. Arlington, Virginia: Aerospace Education Foundation, 2001.

Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. *Grand Strategy for Information Age National Security; Information Assurance for the Twenty-first Century*. Maxwell Air Force Base, Alabama: Air University Press, 1997.

Reference Material

Kay, Maire Weir, ed. *Merriam Webster's Collegiate Thesaurus*. Springfield, Massachusetts: Merriam Webster Inc., 1988.

Morris, William, ed. *The American Heritage Dictionary of the English Language*. Boston: Houghton Mifflin Company, 1973.

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations*, 6th ed. Revised by John Grossman and Alice Bennett. Chicago: The University of Chicago Press, 1996.

Treaties and Protocols

Charter of the United Nations. 1945. in *Basic American Documents.* eds. George B. Huszar, Henry W. Littlefield, and Arthur W. Littlefield, 290-335. Ames, Iowa: Littlefield, Adams, and Company, 1953.

Convention (IV) Respecting the Laws and Customs of War on Land. 1907. in *Documents on the Laws of War*. eds. Adam Roberts and Richard Guelff, 44-59. Oxford: Clarendon Press, 1982.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). 1977. in *Documents on the Laws of War*. eds. Adam Roberts and Richard Guelff, 389-446. Oxford: Clarendon Press, 1982.

INITIAL DISTRIBUTION LIST

1. Air University Library
   Maxwell Air Force Base, AL 36112

2. Colonel E. Wayne Powell
   1463 North Highview Lane #206
   Alexandria, VA 22311

3. Combined Arms Research Library
   U.S. Army Command and General Staff College
   250 Gibbon Ave.
   Fort Leavenworth, KS 66027-2314

4. Defense Technical Information Center/OCA
   8725 John J. Kingman Rd., Suite 944
   Fort Belvoir, VA 22060-6218

5. Major Joanne P.T. Eldridge
   Law Office
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

6. Major Matthew T. Phillips
   Air Force Element
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

1. Certification Date: 31 May 2002

2. Thesis Author: Major Matthew E. Haber

3. Thesis Title: Computer Network Attack and the Laws of Armed Conflict: Searching for Moral Beacons in Twenty-First-Century Cyberwarfare

4. Thesis Committee Members Signatures:

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature:

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).