STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

WHEN DOES AN ACT OF INFORMATION WARFARE BECOME AN ACT OF WAR? AMBIGUITY IN PERCEPTION

BY

COMMANDER MARK B. TREADWELL
United States Navy

19980604 025

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DTIC QUALITY INSPECTED 1

USAWC STRATEGY RESEARCH PROJECT

When Does an Act of Information Warfare Become an Act of War?

Ambiguity in Perception

by

Commander Mark B. Treadwell
United States Navy

Colonel Jack W. Ellertson, USA
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

This page intentionally blank

Abstract

AUTHOR: CDR Mark B. Treadwell, USN

TITLE: When Does an Act of Information Warfare Become an Act of War? Ambiguity in Perception

FORMAT: Strategy Research Project

DATE: 7 May 1998 PAGES: 46 CLASSIFICATION: Unclassified

There is no clear-cut point where information operations can cross over to become the decisive point leading to the start of armed conflict. The use of information operations by nations and individuals could have a significant impact on the public opinion, and, by extension, on the leaders of a nation. Traditional acts of war have been directed towards events that influence a nation's access to, use of, or benefit from *land*. How these concepts may be extended to *information*, either historical (archived or stored) or real-time (systems in use), is problematic at best. This paper addresses how information "warfare" may be interpreted by nations and private citizens in this context.

This page intentionally blank

Table of Contents

Abstract ..... **iii**

Table of Contents ..... **v**

Preface ..... **vii**

List of Figures ..... **ix**

List of Tables ..... **ix**

Abbreviations and Acronyms ..... **xi**

Introduction **1**

The Law of Armed Conflict **3**

Treaties and Conventions 3

On Land, At Sea, and In the Air 5

In Cyberspace 7

Information Operations **8**

Capabilities 10

Weapons 12

Targets 13

A Cyber Act of War **15**

Identification 15

Attack 16

Damage 16

The Public 17

Prior Events 19

Definition 19

Precedents **21**

Legal 21

Historical 24

Cultural 24

Conclusions and Recommendations **26**

Endnotes **27**

Bibliography **31**

Preface

This paper purposely retains a narrow focus and does not address all the aspects of Information Operations (IO). The intent is to take a thoughtful look at a specific aspect of modern operations as the general public of the United States may interpret them. This paper is further restricted by the author's desire to keep the material presented unclassified. Classified material was not used in the research and preparation of this document, and all source materials are openly available.

Due to the sensitive nature of some of the topics, the material presented has been mentioned or proposed by unclassified sources or non-government authors. The examples provided should be considered only as concepts to stimulate thought on "what-if" possibilities.

All interpretations and conclusions are based on the author's twenty years of computer experience, programming, and perusal of computer industry news media.

List of Figures

FIGURE 1: INFORMATION OPERATIONS RELATIONSHIPS ACROSS TIME 9

List of Tables

TABLE 1: LIST OF ABBREVIATIONS AND ACRONYMS USED XI

TABLE 2: INFORMATION OPERATIONS HIERARCHY.....11

Abbreviations and Acronyms

TABLE 1: LIST OF ABBREVIATIONS AND ACRONYMS USED

AFB	Air Force Base
C2W	Command and Control Warfare
CA	Civil Affairs
CERT	Computer Emergency Response Team
CI	Counter-intelligence
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CNN	Cable News Network
COMINT	Communications Intelligence
COMPUSEC	Computer Security
COMSEC	Communications Security
DoD	Department of Defense
EA	Electronic Attack
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HUMINT	Human Intelligence
IA	Information Assurance
INFOSEC	Information Security
IO	Information Operations
IW	Information Warfare
JP	Joint Publication
OASD(PA)	Office of the Assistant Secretary of Defense for Public Affairs
OPSEC	Operations Security
PA	Public Affairs
PCCIP	President's Commission on Critical Infrastructure Protection
PSYOP	Psychological Operations
USC	United States Code

This page intentionally blank

Introduction

> *"All warfare is based on deception.*
> *Therefore, when capable, feign incapacity;*
> *when active, inactivity."*[1]
>
> Sun Tzu

As stated in the title of this paper, there is no known or easily identifiable line across which an information warrior dares not cross unless he desires to incite a future war. Traditional perceptions always attempt to interpret a new situation in old, familiar terms. Each observer will perceive an information operation differently. As the perceptions merge, ambiguity results.

United States Secretary of Defense William Cohen has stated on numerous occasions that the United States must be ready for "asymmetric challenges" that circumvent national strengths, exploit vulnerabilities and threaten both military forces in the field and Americans at home. This asymmetric threat list includes terrorism, environmental sabotage, information warfare, weapons of mass destruction, psychological warfare, and others.[2] Future enemies will use any of these weapons based on the perceived ability to achieve their goal.

Historically, nations have used all weapons available to them, even if distasteful, illegal or immoral. Information warfare weapons are likely to be similar. One of the key measures of success for an information operation may be the inability to discern that an attack has taken place. On the other hand, if subsequently discovered, the use of stealth may be an additional impetus to view the operation as provocative.

In the days of the great European land armies, nations were easily able to identify their aggressors. As the invading force marched across a border, it usually came from a direction that could only be achieved by a single enemy. The enemy wore distinctive uniforms, carried their

country's flag proudly at the fore, and announced their intent to attack beforehand. The matter of identification was never really an issue.

It was done similarly at sea. Tradition had each man-of-war sanctioned by a nation flying that country's ensign, or flag. Indeed, it became a further tradition that each ship would procure a "battle flag" that was many times larger than its every-day flag. Flying these massive colors stirred the souls and emotions of those aboard. It also clearly and proudly identified them to their foe. Battle flags were, and are, flown with the same spirit that led John Hancock to sign the Declaration of Independence with such a bold hand.

Formal means of identifying belligerents applies to an invading army, but does not address how to identify the cyber equivalent. The ability to ascertain rapidly and accurately the actors and their motives in an information attack is the linchpin of success for the remainder of the process. Unfortunately, the nature of many attacks precludes their rapid association with a particular individual or nation-state.

This paper will first discuss the international Law of Armed Conflict to establish a historical basis for a declaration of war. A section follows this on information operations that covers capabilities, weapons and targets. A set of criteria is then explored that interprets the information operations against the Law of Armed Conflict and additional perspectives to develop a checklist that may be applied to an analytical method. Finally, there is a discussion of precedents from the legal, historical and cultural perspectives applying the analytical checklist previously developed.

The Law of Armed Conflict

Much has already been written concerning the Laws of War that will not be repeated here.[3] However, a brief discourse is necessary to set the stage for further discussion. The term "Law of War" is a generally acknowledged term of reference, but not one of clear precision. A war does not need to be in progress to apply the law.

Conventional military attacks on traditional objectives are universally recognized as being under the legal adjudication of international law. This paper will address these common perceptions to illustrate the framework against which we will apply the necessary interpretations when speaking about "information weapons."

Treaties and Conventions

Nations have gone to some lengths and detail to clearly state the process by which they will go to war. The very term itself has changed as the concept has evolved. Initially, the body of international treaties (or conventions) and unwritten or customary law was codified under the umbrella term of the "Law of War."[4] Any treaty must additionally be interpreted with respect to the customary laws in force at the time of signing that were not included in writing.

In acknowledgement that nations typically no longer declare war on each other, but do still continue to engage each other militarily, this body of law has come to be referred to as the "Law of Armed Conflict."[5] What exactly is "armed conflict?" The various Geneva and Hague conventions do not define the term, and a formal dictionary definition is not available, but an amalgam definition could be:

> *armed* "furnished with arms (weapons) or armor; fully equipped for war, … [in a phrase, it] refers to the persons or power making the demonstration …"[6]

conflict "an encounter with arms; a fight, battle; martial strife."[7]

"Armed conflict" has a nicer connotation than the true violence of war. In keeping with the concept of nation-states being the only entities that formally go to war, armed conflict may occur "wherever regular armed forces of a nation-state engage the regular armed forces of an enemy nation-state."[8] This definition is somewhat limited, and will be expanded in the next section.

The use of armies to engage in war on other nations has been codified in both tradition (custom) and convention. The Third Hague Convention Relative to the Opening of Hostilities is very clear that nations "... recognize that hostilities between themselves must not commence without previous and explicit warning, in the form either of a reasoned declaration of war or of an ultimatum with conditional declaration of war."[9] The United States' last declared war was against Germany and Japan in World War II. The 1991 Gulf War was not formally declared as stipulated in the Convention, although there was an ultimatum. This tendency has limited the perceived applicability of the Law of Armed Conflict to war today.

The application of tradition to the start of conflict is less clear. Mostly, it concerns events that have no precedent, or events that set a precedent which was generally concluded by the international community to be inappropriate. An example of this is a much larger nation attacking a smaller one with the intent of eradicating it. The fight is perceived to be an unfair one, even though military experts will tell you to never pick a fair fight and always try for overwhelming superiority.

International conventions concerning the laws and customs of war on land have been consistent in their identification of belligerents under a State. Individuals must either be a member of the State's armed forces or fill the following conditions:

- commanded by a person responsible for his subordinates;
- having a fixed distinctive sign recognizable at a distance;
- carrying arms openly;
- conducting their operations in accordance with the laws and customs of war.[10]

These formal means of identifying belligerents applies to an invading army, but does not address how to identify the cyber equivalent.

On Land, At Sea, and In the Air

International conventions have consistently dealt with war "on land" and "at sea." This is easily understood, since people and nations were concerned with physical possession and use of territory. This separation worked well in the agrarian and industrial ages since the products of the land and their usefulness to the land's occupants represented real value. An enemy attack on an area, restriction, damages or occupation was considered an act of war.

This was easily extended to the seas. The world's oceans were divided into "international waters" and "territorial waters;" territorial waters were an extension of a sovereign nation's land area.[11] Any incursion into territorial waters, either on the surface or beneath it, was treated as an incursion on land.

With the invention of the airplane, international rules were extended to cover air space, based on rules governing the sea. Thus, the link to a nation's land was retained and reinforced. A sovereign nation thus has control over the air, sea and land within its boundaries.

The United Nations Special Committee on the Question of Defining Aggression completed its work in 1974. The acts defined by the Committee equate quite well with the traditionally accepted acts of war.

ARTICLE 1. Aggression is the **use of armed force** by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in the Definition.

ARTICLE 2. The **first use** of armed force by a State in contravention of the Charter of the United Nations shall constitute *prima facie* evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.

ARTICLE 3. Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with Article 2 qualify as an act of aggression:

(a) The **invasion or attack** by the armed forces of a State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State of part thereof;

(b) **Bombardment** by the armed forces of a State against the territory of another State or the use of weapons by a State against the territory of another State;

(c) The **blockade** of the ports or coasts of a State by the armed forces of another State;

(d) An attack by the armed forces of a State on the land, sea or air forces, marine and air fleets of another State;

(e) The use of the armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in said territory beyond the termination of the agreement;

(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of **aggression against a third State**;

(g) The sending by or on behalf of a Sate of **armed bands, groups, irregulars or mercenaries**, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

ARTICLE 4. The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter.[12]

The definition that reinforces the land equivalence for an act of war will be applied to information warfare. Our new definition of armed conflict can now be stated as being "wherever the sanctioned forces of a nation-state engage the sanctioned forces of an enemy nation-state."

In Cyberspace

Carl von Clausewitz abstractly described how war originates:

> "Essentially, the concept of war does not originate with the attack, because the ultimate object of attack is not fighting: rather, it is possession. The idea of war originates with the defense, which does have fighting as its immediate object, since fighting and parrying obviously amount to the same thing. ... The side that first introduces the element of war ... is also the side that establishes the initial laws of war. That side is the *defense*. ... The defender must establish ground rules for his conduct even if he has no idea what the attacker means to do, ... The attacker, on the other hand, so long as he knows nothing about his adversary, will have no guidelines on which to base his use of [force]."[13]

Given Clausewitz's definition of the defender's perception of the attacker's desire for possession, does possession equate to electronic trespass and manipulation? Where is the line of sovereignty drawn? Can sovereignty be extended into cyberspace?

If one compares cyberspace to *land*, the earlier discussion on sovereign territory and the Law of Armed Conflict can be extended logically to computer systems and their infrastructure. A simple definition of "attack" would be the entry or attempted entry into a system without authorization or for illegal use. If an agent, whether nationally sponsored or an individual, conducts an attack on a system that may have a significant impact on the national security or normal operation of systems or infrastructure within the land territory of a nation, it can be considered an attack by an armed force on land. This is a significant determination, and it must be tempered by the relative significance of the attack as discussed below.

Central to the application of the Law of Armed Conflict to Information Warfare is identification of the combatant and the neutral. In the cyber realm, a combatant is the individual who is actually conducting the electronic attack, regardless of location.

Information Operations

> *"Generally in war the best policy is to take a state intact; to ruin it is inferior to this. ... To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."*[14]
>
> Sun Tzu

Over time, there has been an increasing sophistication and precision in terminology with regard to information operations (IO). It has occurred as understanding of the subject area has matured. In the earliest days, it was "password security." This has morphed and expanded to "computer security," then "information systems security," to "information protection," to "information assurance," to "information warfare," and now "information operations."[15] Later concepts subsumed some of these as the scope of consideration and understanding expanded.

To conduct any type of information operations, two basic requirements must be met: access to the system and an understanding of how it works. In the case of a radar, knowledge of the antenna location and operating frequency permit jamming, a practice that has occurred almost since the system was invented. Military combat computer systems are more difficult to attack due to secure communications and unique programming, making them tempting targets for hackers who cannot resist a challenge. By extension, it is almost impossible to assess whether the attack is successful, except by watching the response or listening to intercepted communications. This is true for either the radar example or the computer attack.[16]

Information operations are best defined in Joint Publication 3-13:

> "IO involves actions taken to **affect adversary information and information systems while defending one's own information and information systems**. IO apply across all phases of an operation throughout the range of military operations, and at every level of war. Information Warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific

objectives over a specific adversary or adversaries. **Defensive IO activities** are conducted on a continuous basis and are an inherent part of force deployment, employment, and redeployment across the range of military operations. **IO may involve complex legal and policy issues** requiring careful review and national-level coordination and approval."[17]

This definition presumes operations are in progress prior to the commencement of hostilities. An opposing force can be reasonably expected to do the same. The flow of information operations is illustrated in Figure 1.

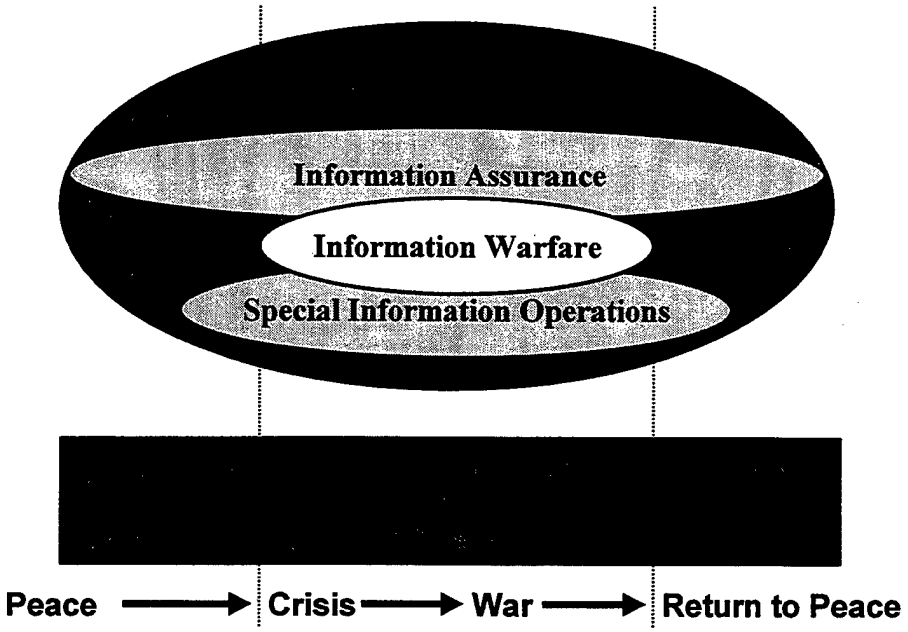

FIGURE 1: INFORMATION OPERATIONS RELATIONSHIPS ACROSS TIME[18]

It can be seen that information operations are intended to be in progress just before and during the crisis stage preparatory to war. The magnitude and significance of these operations will be tailored to the adversary. The heightened public awareness that coincides with any international crisis will magnify the impact of information operations revealed publicly. A news media frenzy will likely erupt, illustrating that the drive for excellence in journalistic endeavors is alive and well.[19]

The attackee's control of how these information operations are presented to the world news media may be as vital as the strategic effect of the operation itself. The initial public interpretation ("spin") attached to the information operation will be an important aspect of the operation's comparison with it being an act of war. The attackee must identify the attacker and promote indignation that the attacker would carry out an IO attack. Once reliably identified, the attacker must justify the attack according to the Law of Armed Conflict.

Capabilities

Military forces use offensive information operations across the full range of operations to target an enemy's decision making process. To be effective, without being excessive, they must have clearly established goals, support the overall national and military objectives, and include identifiable measures of success. The selection and subsequent employment of offensive information operation capabilities must remain appropriate to the situation and consistent with U.S. strategy and objectives. The actions must be permissible under the Law of Armed Conflict, consistent with any applicable domestic or international laws, and be in accordance with any applicable rules of engagement.[20]

One Chinese author considers a full spectrum of information operations as being necessary beforehand to the application of firepower, specifically with respect to precision guided munitions and the tracking, aiming, reconnaissance, and fire control of guns.[21]

The hierarchy of information operations is illustrated diagrammatically in Table 2.

TABLE 2: INFORMATION OPERATIONS HIERARCHY[22]

				JP
Information Operations				3-13
Offensive	C2W	EW	EA	3-51
			EP	3-51
			ES	3-51
		PSYOP		3-53
		OPSEC		3-54
		Military Deception		
		Physical Destruction		
	CNA			
	Support	PA		1-07
		CA		3-57
Defensive	OPSEC			3-54
	EW	EA		3-51
		EP		3-51
		ES		3-51
	Education, Training, Awareness			
	Intelligence Support			
	Counter-deception			
	Counter-PSYOP			
	CI			2-02.1
	PA			1-07
	Command Information			

Information operations within the realm of traditional military activities are excluded from the realm of "covert action," as is discussed later. This opens up large areas of the offensive information operations spectrum. This is especially relevant for Command and Control Warfare (C2W). As a subset of offensive information operations, many C2W techniques are considered "traditional" and still fit outside the covert realm.

The National Command Authority may desire to retain approval authority for certain information warfare capabilities that could have a significant impact on an enemy's civilian populace. As long as the targeting decision meets the legal analysis of: "(1) whether to apply the

Law of Peace or the Law of War; (2) the legitimacy of the target under international law and the Law of Armed Conflict; and (3) the procedural requirements for obtaining appropriate approval for individual targets or plans,"[23] the use of offensive information warfare is lawful.

Weapons

In exercises, strategic information warfare has had seven defining features: low entry cost, blurred traditional boundaries, an expanded role for perception management, a new strategic intelligence challenge, formidable tactical warning and attack assessment problems, difficulty of building and sustaining coalitions, and vulnerability of the United States homeland.[24] These affect and influence the development of this new, cyber weapon technology. Three of these seven are of greater significance.

First, since interconnected computer systems allow access from almost anywhere on the planet, the *strategic intelligence challenge* to identify the location cannot be based on the location of the attacking equipment. Instead it must use a deeper analysis of capability and intent to locate the guiding and directing influence that is controlling coordinated attacks. This does not remove the requirement to trace and locate the actual weapon directors, the attackers, once they launch the attack.

Second, the remote location of the "weapon site" almost guarantees a lack of *tactical warning*, and greatly compounds the difficulty of assessing the attack since cyber weapons have the longest range in the world. A central clearinghouse, akin to a tactical command post in the field, is mandatory in order to reduce time in collating reports. Nation-states have been fortunate in that hacking "thrill seekers" seem to be the most common deliberate attack so far.[25] Nation-

states themselves are likely staying away from massive, coordinated attacks with no strategic goal in order to avoid the climate of "mutually-assured annoyance"[26] it would likely guarantee.

Third, the major defining feature is the *vulnerability of the U.S. homeland.* Catch phrases such as "in the cyber dimension there are no boundaries,"[27] "information warfare has no front line,"[28] and "digital Pearl Harbor"[29] have become synonymous with the threat these cyber weapons pose. Most people in the U.S. have little concern for this fact as long as it does not affect their lives. When the impact does occur, the public's response will be swift and indignant.

The U.S. arsenal today contains at least two hardware information weapons. The Navy Tomahawk cruise missile can be armed with a special warhead that sprays fine, specially treated wires over outdoor electrical grids. The Air Force Wind Corrected Munitions Dispenser can spray a cloud of minute carbon fibers that coat the surface and internals of antennas and electronic equipment, rendering them useless. Two possible future systems involve the use of high-powered microwave generators and lasers.[30]

Software weapons are freely available on the Internet and rely on known security problems to exploit weaknesses in improperly configured systems. The very standards that make the Internet work are its weakness.[31] Part of this is due to the widespread use of free server software that had bugs and programming holes. While corrected over time, systems administrators continued to use earlier versions, mostly because of a "if it works, don't mess with it" philosophy. New systems are configured by copying old setups, propagating the problem.

Targets

President Clinton stated that "Our responsibility is to build the world of tomorrow by embarking on a period of construction—one based on current realities but enduring American

values and interests."[32] These enduring national interests have a strong influence in defining targets of interest for information attacks.

For the public sector, Presidential Executive Order 13010 developed a list of "certain national infrastructures [which] are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government."[33] The Order additionally established the President's Commission on Critical Infrastructure Protection (PCCIP).

The PCCIP evaluated these infrastructures, assessed their vulnerabilities, and deliberated assurance alternatives. While a physical attack was considered, the Commission "focused more on cyber issues than on physical issues, because cyber issues are new and not well understood."[34]

Government computer systems are an obvious target, in particular those of the military services. Hostile nation-states will be interested in these targets for strategic or tactical information. Thrill-seeking hackers will be in it for the challenge. Terrorist or hate groups as well as nation-states will be interested in causing disruption or loss.

What will be attacked? The system must be accessible, understandable, and vulnerable. Special purpose or older systems with uncommon interfaces are the least vulnerable. This is particularly true if access must be via a dial-up modem. Internet-connected systems running standard software that identifies itself are much more vulnerable.

A Cyber Act of War

A *threat* is traditionally identified as a *capability* linked to *hostile intent*. This link is vital to the traditional function of the intelligence services, since they could see who had the capability and evaluate intent to determine threat level. Cold War weapons were large, expensive, took years to develop and required the assets of a nation to support. Today, the threat need not be from a nation-state. The weapons are no longer expensive and frequently have legitimate peacetime applications.

Hostile attempts to damage, misuse, or otherwise subvert critical infrastructures are the primary focus of a national policy, since natural disasters, poor design and accidents may occur at any time. The following criteria are intended to be the broad categories that are used in determining the severity of a hostile information operation. The criteria also show how IO could be the pivotal event leading to war.

Identification

The ability to ascertain rapidly and accurately the actors and their motives in an information attack is the linchpin of success for the remainder of the process. Unfortunately, the nature of many attacks precludes their rapid association with a particular individual or nation-state.

Beyond accidents and negligence, threats to computer systems run from prankish hacking at the low end to organized, synchronized attacks at the high end. The basic tools used for an attack are widely available.[35] The PCCIP identified that the most worrisome computer threat is from an insider who has legitimate, authorized access to a computer system or network. These insiders may be either willing or unwitting.[36]

The association of a computer location or user to a nation-state requires a parallel effort of both communications intelligence (COMINT) and human intelligence (HUMINT) resources. If the attack is being committed by proxy, HUMINT and COMINT may be the only means to determine the relationship between the attacker and the sponsor.

Attack

The PCCIP identified two broad categories of threats: physical and cyber. The physical threats such as bombing or malicious entry are very well understood and have well-proven means for protection and surveillance. A cyber attack is relatively new, not well understood or fully appreciated.

The origin of a cyber attack will influence who has jurisdiction and responsibility, as well as who may pursue information on the perpetrator(s) based on current United States Code. A physical attack with its attendant destruction or disruption will be handled by domestic law enforcement.

Damage

Executive Order 12958 provides a guideline to establish a method to measure the significance of an information attack, using the classification levels for national security information.[37] Using this Executive Order as a guide, the following terminology may be used to describe the severity or magnitude of an information attack:

- TYPE 1: The attack could be evaluated to have caused *nuisance or inconvenience* to the defense or economic security of the United States.
- TYPE 2: The attack could be evaluated to have caused *damage* to the defense or economic security of the United States.

- TYPE 3: The attack could be evaluated to have caused *serious damage* to the defense or economic security of the United States.
- TYPE 4: The attack could be evaluated to have caused *exceptionally grave damage* to the defense or economic security of the United States.
- TYPE 5: The attack could be evaluated to have caused *critically vital damage* to the defense or economic security of the United States.

These severity criteria are arbitrary, but may be useful since they equate to an already familiar and well-used method of classification.

Evaluation of the damage must be done in three ways. First, those who directly operate the attacked system must determine exactly what was done, how it was accomplished, and the estimated time and cost for recovery. Second, higher level supervision must evaluate peripheral or cascading damage and what impact the attack will have. Third, the highest manager must assess the psychological and, potentially, emotional impact of the attack.

The Public

The "public" involved with an information operation is present in both of the involved nations. How the public forms an impression and interprets an information operation is largely dependent upon how the details are presented. This may presume attribution of the attack to a specific State. Perception is one of the primary forces driving public sentiment, especially with a worldwide electronic audience.

First, an official press conference should include an official acknowledgement (or refutation) of the event, supporting information, and a statement of policy. All should be

prepared before hand; classified operations could end up with extremely public consequences that must be anticipated.

Second, reporters' background knowledge of the subject and how it influences their follow-on questions would allow an expanded explanation of the government's actions. Historically, reporters in the United States have gone for the dramatic and exciting rather than the boring and factual. They frequently seem to approach reporting as if every action is illegal or bordering on illegality. If a reporter is operating on the edge of or beyond his realm of knowledge, the possibility of rampant speculation, willingness to believe and report to the public goes up exponentially. Off-the-record background briefs on general technology and policies as well as the legal basis are required.

Third, a news organization usually performs follow-up analysis of the information with one or more experts. Since the general public cannot always be completely informed on the background prior to an operation, these individuals provide the context that the public lacks. It would be especially important to detail the aspects of international law that cover the attack.

Unless the attacker is a nation-state, the attack will probably be completely anonymous. The non-state actor may reveal the attack to a news organization by facsimile, letter or email. The attacked government may be exercising news conference damage control with minimal or no confirmed details. Since government officials rarely desire to comment without complete information, this leaves the interpretation of the event open to speculation rather than informed analysis. Additionally, the FBI may restrict the release of details if there is a suspicion that a United States person may be involved with the event.

Prior Events

Prior events have a direct and major impact on perception. The assassination of Archduke Ferdinand in Sarejevo was the culminating act in a long series of events that precipitated World War I, but preceding events were what truly forced the war. United States bombers attacked downtown Tripoli in 1986 without a war. Similarly, Israel's attack on the Iraqi Tammuz Osiraq reactor in June 1981, while bringing condemnation, did not precipitate a conflict. In both cases, an argument could be made that the precursors for war were absent and that additional forces were at work besides just the bombs on target.[38]

A nation's people build up an impression over time. That impression molds new information into opinions. The opinions are expressed in the short-term via polls, questions and speeches. They are expressed over the long-term via sanctions, elections, and law. Specific events must be assessed against this background to evaluate effect.

Definition

How do you apply the above criteria to determine if the information operation equates to an act of war? The following discussion provides a checklist approach. It must be emphasized that any analysis must be tempered with the informed opinions of people knowledgeable with all the facts of the case.

The effective determination of a act of cyber war will be based on a combination or checklist version of the previously listed areas. Each will have to be evaluated, all combined, and then a determination made. The following sequence is one possibility.

- If a person conducting an attack can be reliably connected with a nation-state that is a threat (harbors known hostile intent and known capability) to the U.S.;

- and the attack is made on systems or infrastructure within sovereign U.S. territory or on military systems anywhere;
- and the damage is judged by a majority of people to be of sufficient breadth and magnitude (equivalent to a Type 5 attack described above);
- and the general public, as determined via polls, news organizations or government officials, determines the attack to demonstratively hostile to the U.S.;
- and prior events indicate a continuing program of hostile acts with probable future hostile intent;
- then the attack committed may be judged sufficient to be declared an act of war.

This confluence of events and judgements should be rare, since there is little or no precedent on which to form a judgement. The ultimate way to judge if something was an act of war is to later see if a war is fought because of it.

Precedents

Legal

The United States military is not enjoined from engaging in overt intelligence gathering missions. Normal international laws and rules apply. These operations are frequently required to support the military's traditional intelligence and counterintelligence requirements. Covert military actions are quite different, with peacetime information operations against foreign targets coordinated in an interagency process.[39]

The following paragraphs address the authoritative documents with respect to covert operations, with emphasis on their information operations applicability. Generally, their limited guidance indicates that in time of peace, the military is primarily intended to provide a supporting role to the Central Intelligence Agency (CIA), or, in a significantly more limited degree, to the Federal Bureau of Investigation (FBI). These relationships change dramatically, however, when one of two events occur: the United States is engaged in a war, or a period of crisis, requiring a Presidential report to Congress pursuant to the War Powers Resolution; or a Presidential Finding is made authorizing the Department of Defense to take covert actions which are intended to achieve a particular objective.[40]

The laws that cover covert information operations are in Title 50, Section 413b of the U.S. Code. This statutory framework requires that the President submit a written Finding to Congress describing why a particular action is necessary to support identifiable foreign policy objectives, and why the action is important to the national security of the United States. This process must be complete before the President can authorize any United States Government entity to engage in covert action.[41]

50 USC 413b defines "covert action" as

> an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include —
>
> (1) activities the primary purpose of which is to require intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
>
> (2) traditional diplomatic or military activities or routine support of such activities;
>
> (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such agencies; or
>
> (4) activities to provide routine support to overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.[42]

Presidential Executive Order 12333 "United States Intelligence Activities" expands on the statutory language. This document is binding on all elements of the Executive Branch and identifies the division of intelligence responsibilities between the CIA, Department of State, Department of the Treasury, DoD, Department of Energy and the FBI. The CIA is designated as the only United States Agency authorized to conduct "special activities" (i.e., covert actions) except if one of the two events described above occurs. The Department of State is tasked to overtly collect information relevant to United States foreign policy concerns. The Department of the Treasury is tasked to overtly collect foreign financial, monetary and economic information. The DoD is directed to respond to the tasking of the Director of Central Intelligence; is required perform its traditional missions to collect, produce, and disseminate military and military-related intelligence and counterintelligence; and is the specified lead agency in conducting signals intelligence through the National Security Agency. The Department of Energy is tasked to overtly collect information on foreign energy matters. The FBI is tasked to conduct and

coordinate internal counterintelligence activities, conduct external counterintelligence activities coordinated with the CIA, and collect internal foreign intelligence.

Executive Order 12333 also specifically prohibits all executive agencies from having undisclosed participation in organizations within the United States without agency and Attorney General approval. This participation can only be undertaken on behalf of the FBI as part of a lawful investigation, or when the organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.[43]

Although it does not address covert actions, the DoD Law of War Program stipulates that it is the policy of the Department that the Law of War and the obligations of the United States Government under that law are to be observed and enforced by the United States Armed Forces. It further defines the Law of War as "[encompassing] all international law with respect to the conduct of armed conflict, binding on the United States or its individual citizens, either in international treaties and agreements to which the United States is party, or applicable as customary international law."[44]

Chairman of the Joint Chiefs of Staff Instruction 3210 provides additional specific direction on information operations. It requires National Command Authority approval with an interagency coordination process prior to the employment of offensive information operations capabilities in peacetime.[45]

These laws and regulations adequately address the conduct of information operations that may lead to another nation-state interpreting an operation against them as being an act of war. This places the oversight at the Presidential level with the Finding being the vehicle to ensure that the Congress remains informed.

Historical

Historical precedents made public to date have been small-time hacking incidents attributable to single or small groups of hackers seeking recreational thrills. With each event, the public gets another bit of information to form an impression on the U.S. vulnerability and perceived level of damage caused by the attack. Typically, the targets have been non-sensitive or unclassified systems. There has not been a great impression of vulnerability or lasting consequences.

Additionally, there has been no public evidence of a single source collating the information gained from multiple attacks. According to published accounts, the authorities have found the direct perpetrator, but have infrequently traced a behind-the-scenes director or mentor.

Cultural

This is much more difficult to explore since cultures and points of view differ greatly. Social mores are so significantly different that only the U.S. perspective will be reviewed.

A cultural view of an act of war will be based on past actions and incidents. The 1990 Iraqi invasion of Kuwait was globally recognized as an act of war based on the impression of a larger, stronger nation attacking a smaller, weaker one with little or no warning. The public's view of the event would have been significantly different had Iraq focussed its attack only on Kuwaiti computer networks, telephone systems, and broadcast facilities. With no tanks in the streets, fires, clouds of smoke, or deaths, people would have been less impressed. They would have had nothing tangible to evaluate and compare the impact against.

This requirement for the public to have something tangible is key to understanding the magnitude and direction of its reaction. Often, the "public's" reaction is that of the press or its

elected leaders. Both are the most immediately available for comment in this CNN information age. Polls and surveys take longer to assemble and can vary widely based on how informed the survey participants are and their depth of understanding of background or key preceding events.

With this cultural filter in place, information can be presented with an inaccurate or biased "spin" that may only confuse the issue. This type of media event has been present in several Washington political crises. Each time, polls and surveys show public opinion to be much more conservative than the salacious news organizations have believed (or desired).

Conclusions and Recommendations

There is no firm set of criteria to judge an information operation to determine if it constitutes an act of war. Such a magical list would be wonderful, but it is not achievable due the inherent ambiguity in cyber attacks and the attendant necessity to rely on perception to judge an act as warlike. With so many people involved, all with different opinions, consensus building in the heat of the battle may be impossible. In the U.S., this is further complicated in that only Congress may declare war; this is an event that appears to have drifted out of vogue.

Some things, however, can be done. With adequate information, a response in kind can be launched. Worldwide publicity can be invoked against the attacker with the U.S. interpretation dominant. This interpretation can include the phrase "act of war" to generate the impression in the target audience of the perceived severity without actually declaring war. This follows well with the Law of Armed Conflict's Principle of Military Necessity as well as proportionality.

Escalation should be avoided. A physical weapon of mass destruction may never equate to a cyber weapon of mass disruption. Such a leap of intuition will come only after major cyber attacks have been launched and the public can see and evaluate the results to form their opinion.

5813 words

Endnotes

[1] Sun Tzu, The Art of War, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 66.

[2] Secretary Cohen articulated this list over a series of speeches from 27 March through 30 May 1997. All are available as DoD OASD(PA) News Releases (Reference Number 142-97, remarks as delivered to the Navy League Exposition on 27 March 1997; Reference Number 200-97, remarks as delivered to the Western Hemisphere Symposium on 15 April 1997; Reference Number 258-97, remarks prepared for delivery to the Center for Strategic and International Studies on 22 May 1997) or as DoD News Briefings (Media availability following the Secretary's acceptance of the Bull Simon's Award, McDill AFB, FL on 16 April 1997; Breakfast meeting, Los Angeles Chamber of Commerce, Loyola Marymount University, Westchester, CA on 30 May 1997). All are available from <http://www.defenselink.mil/> with a search for "information warfare;" Internet; accessed on 11 October 1997.

[3] The Law of Armed Conflict includes the principles of military necessity, humanity and chivalry. For a discussion of these, see Richard W. Aldrich, The Legal Implications of Information Warfare, USAF Institute for National Security Studies Occasional Paper 9 (United States Air Force Academy, CO: n.p., April 1996) 6-18; Karl Kuschner, Major, USAF, "Legal and Practical Constraints on Information Warfare," available from <http://www.cdsar.af.mil/cc/kuschner.html>, Internet, accessed 19 December 1997; U.S. Department of the Air Force, Office of the Staff Judge Advocate, Moody AFB, "Legal Aspects of Information Warfare," available from <http://www.moody.af.mil/wg/ja/AOR/opsinfo.htm>, Internet, accessed 19 December 1997; U.S. Department of the Air Force, Office of the Staff Judge Advocate, Moody AFB, "Law of Armed Conflict," available from <http://www.moody. af.mil/wg/ja/AOR/opsloac.htm>, Internet, accessed 16 February 1998; and U.S. Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, Joint Staff research report prepared by Science Applications International Corporation (Washington, D.C.: GPO, 4 July 1995).

[4] Department of the Army, The Law of Land Warfare, Field Manual 27-10 (Washington, D.C.: U.S. Department of the Army, 18 July 1956) with Change One dated 15 July 1976, 3-4.

[5] The phrase "armed conflict" was specifically chosen over the word "war" because of its broader scope. The 1949 view of conflict was completely unaware of the implications of this expansion in view of the Tofflers' Third Wave.

[6] Oxford University Press, The Oxford English Dictionary, Second Edition, Volume I (Oxford: Clarendon Press, 1989) 634-636.

[7] Ibid., Volume III, 713.

[8] Aldrich comes to a similar definition, but by a different method. The "engage" in the definition is intended to imply a physical confrontation.

[9] Hague Convention No. III Relative to the Opening of Hostilities, Article 1. Quoted in U.S. Department of the Army, Treaties Governing Land Warfare, Pamphlet 27-1 (Washington, D.C.: U.S. Department of the Army, 7 December 1956), 2.

[10] Geneva Convention (III) Relative to the Treatment of Prisoners of War of 12 August 1949, Article 4. Reprinted in Dietrich Schindler and Jirí Toman, eds., The Laws of Armed Conflicts: A Collection of Conventions, Resolutions and Other Documents, Second Edition (Rockville, MD: Sijthoff & Noordhoff, 1981), 363. This identification is identical with the first two Geneva Conventions signed on the same date (Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field [Article 13], and Convention

(II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea [Article 13]). The identification of a belligerent was initially codified at the Brussels Conference of 1874, with further refinement in the Oxford Manual of 1880 (Article 2) and the Hague Conventions on Land Warfare of 1899/1907 (Annex Article 1).

[11] The 1982 Law of the Sea Convention allowed coastal nations to lawfully establish the maximum distance offshore for territorial waters as twelve nautical miles. Anecdotally, twelve miles is the approximate distance at which someone standing at the waterline on shore may visually sight a ship. The United States claims a twelve-mile territorial sea and recognizes the right of all coastal and island nations to do likewise. Additionally, the United States has a continuing Freedom of Navigation Program to challenge territorial claims in excess of twelve nautical miles. Additional details may be found in Horace B. Robertson, Jr., ed., The Law of Naval Operations, U.S. Naval War College International Law Studies, Volume 64 (Newport, RI: Naval War College Press) 456-473.

[12] Yearbook of the United Nations 1974, 28 (United Nations: Office of Public Information, 1977), 847. Cited in Howard S. Levie, The Code of International Armed Conflict, vol. 1 (New York: Oceana Publications) 51-53. Original source is United Nations General Assembly Resolution 3314 (XXIX) of 14 December 1974. Emphasis added. Of note, this resolution was adopted without a vote. In the Report of the Special Committee [of the General Assembly of the United Nations] on the Question of Defining Aggression, the following important statement appears. "With reference to Article 3, subparagraph (b), the Special Committee agreed that the expression 'any weapons' is used without making distinction between conventional weapons, weapons of mass destruction and any other kind of weapon." This has an interesting connotation for information warfare weapons.

[13] Carl von Clausewitz, On War, ed. and trans. by Michael Howard and Peter Paret. (Princeton, NJ: Princeton University Press, 1976), 377. Italics are from the original.

[14] Sun Tzu, 77.

[15] Michael A. Dornheim, "Bombs Still Beat Bytes," Aviation Week and Space Technology 148, no. 3 (19 January 1998): 60.

[16] Ibid.

[17] U.S. Department of Defense, Joint Doctrine for Information Operations, Joint Publication 3-13, Preliminary Coordination Draft (Washington, D.C.: U.S. Department of Defense, 28 January 1998), I-1. Emphasis is in the original.

[18] Ibid., I-4.

[19] The impact of this journalistic one-upmanship cannot be discounted. When nations are in the rapid thrust and parry stages before a conflict begins, the media can exert significant influence on a nation's head of state or head of government. The Cable News Network effect can come into play where the media is providing the bulk of the information on the most recent events vice the nation's intelligence assets. This has been evident several times since the 1991 Gulf War.

[20] JP 3-13, II-1

[21] Chang Mengxiong, "Weapons of the 21st Century," China Military Science (Spring 1995). In Michael Pillsbury, trans. and ed., Chinese Views of Future Warfare, Washington, D.C.: National Defense University, 1997.

[22] JP 3-13, II-4 – II-8 and III-6 – III-9; and U.S. Department of Defense, Compendium of Joint Publications, Joint Publication 1-01.1 (Washington, D.C.: U.S. Department of Defense, 25 April 1995), ii.

[23] Stephen A. Rose, Captain, JAGC, USN, Commander in Chief United States Atlantic Command, Staff Judge Advocate (J02L), "Legal Aspects of Offensive Information Warfare --- Information Memorandum," memorandum for information warfare game participants, Norfolk, VA, 16 January 1996, 1.

[24] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New face of War," Parameters XXVI, no. 3 (Autumn 1996): 81-91. Also available from <http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm>; Internet; accessed 12 October 1997. From the original: Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War" (Santa Monica, CA: RAND, 1996). The full text of the study is available from <http://www.rand.org/publications/MR/MR661/MR661.pdf>; Internet; accessed 12 October 1997.

[25] Ibid.

[26] Dornheim, 60.

[27] Robert T. Marsh, "Critical Foundations: Protecting America's Infrastructures," The Report of the President's Commission on Critical Infrastructure Protection (Washington, D.C., 13 October 1997), vii.

[28] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, 89.

[29] Brian C. Lewis, "Information Warfare," available from <http://www.fas.org/irp/eprint/snyder/infowarfare.htm>, Internet, accessed 10 October 1997. The original source is Winn Schwartau in his 1991 testimony before Congress.

[30] David A. Fulghum, "New Weapons Slowed By Secrecy Clampdown," Aviation Week and Space Technology 148, no. 3 (19 January 1998): 54.

[31] The Computer Emergency Response Team (CERT) of Carnegie Mellon University is the federally funded central clearinghouse for computer network attack (CNA). Their web site offers a tremendous amount of information on how to correct known weaknesses using the CERT alert archives, security improvement technical tips, security improvement modules, checklists and program tools for improving site security. Some of the known types of attack listed include File Transfer Protocol (FTP) port attacks, anonymous FTP abuses, SYN denial of service attacks, Internet protocol spoofing (masquerading), email spoofing, and email spamming. These are available at <http://www.cert.org/>; Internet, accessed 24 February 1998.

[32] William J. Clinton, "A National Security Strategy for a New Century," May 1997, i.

[33] Executive Order 13010, "Critical Infrastructure Protection," 15 July 1996, as amended by Executive Order 13025 of 13 November 1996, Executive Order 13041 of 3 April 1997, and Executive Order 13064 of 11 October 1997; Introduction. The text of Executive Order 13010 in its full amended form is available from <http://www.pccip.gov/eo13010.html>; Internet; accessed 5 February 1998.

[34] Marsh, 15.

[35] Ibid. The required tools include a computer, modem, telephone line or network connection, and user-friendly hacker software. The last item has significantly reduced the level of knowledge required.

[36] Ibid. The willing insider may be a disgruntled employee. The unwitting insider may be someone who is convinced by an outsider to carry in a disk with hidden or disguised code that will permit later outside access. A favorite container of this type of hidden code is a screen saver.

[37] Executive Order 12958, "Classified National Security Information," 17 April 1995. Available from <http://library.whitehouse.gov/Search/Query-ExecutiveOrders.html> with a search for Executive Order Number 12958; Internet; accessed 6 February 1998. Section 1.3 of the Order provides for information classification levels. "'Top Secret' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe." This equates to a Type 4 attack in severity or significance. Unauthorized disclosure of "Secret" material could be expected to cause *serious damage*. This equates to a Type 3 attack in severity or significance. Unauthorized disclosure of "Confidential" material could be expected to cause *damage*. This equates to a Type 2 attack in severity or significance. A Type 1 attack was defined to allow for events that were insignificant or were defeated.

[38] Winn Schwartau, "Ethical Conundra of Information Warfare," available from <http://www.infowar.com/mil_c4i/iw_thics.html-ssi>; Internet; accessed 18 December 1997. This piece includes some additional interesting speculation.

[39] Stephen A. Rose, Captain, JAGC, USN, Commander in Chief United States Atlantic Command Staff Judge Advocate (J02L), "Legal Aspects of Peacetime Information Warfare --- Command and Control," memorandum for information warfare wargame participants, Norfolk, VA, 29 January 1996. 1-2.

[40] Presidential Approval and Reporting of Covert Actions, U.S. Code, Title 50, sec. 413b (1994).

[41] Ibid.

[42] Ibid.

[43] Executive Order 12333. "United States Intelligence Activities." 4 December 1981. Part 1. U.S. Code. Title 50, sec. 401 (1994).

[44] U.S. Department of Defense, DoD Law of War Program, Directive 5100.77. (Washington, D.C.: U.S. Department of Defense, 10 July 1979), 1-2.

[45] Rose, "Legal Aspects of Peacetime Information Warfare --- Command and Control," 2.

Bibliography

BOOKS:

Baocun, Wang and Li Fei. "Information Warfare," excerpted from articles in Liberation Army Daily, 13 and 20 June 1995. In Pillsbury, Michael, trans. and ed., Chinese Views of Future Warfare, Washington, D.C.: National Defense University, 1997.

Clausewitz, Carl von. On War. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Jincheng, Wei. "Information War: A New Form of People's War," excerpted from the Military Forum column, Liberation Army Daily, 25 June 1996. In Pillsbury, Michael, trans. and ed., Chinese Views of Future Warfare, Washington, D.C.: National Defense University, 1997.

Levie, Howard S. The Code of International Armed Conflict. Vol. 1. New York: Oceana Publications.

Mengxiong, Chang. "Weapons of the 21st Century," China Military Science (Spring 1995). In Pillsbury, Michael, trans. and ed., Chinese Views of Future Warfare, Washington, D.C.: National Defense University, 1997.

Oxford University Press. The Oxford English Dictionary. Second Edition. Oxford: Clarendon Press, 1989.

Pufeng, Wang, Major General. "The Challenge of Information Warfare," excerpted from China Military Science, Spring 1995. In Pillsbury, Michael, trans. and ed., Chinese Views of Future Warfare, Washington, D.C.: National Defense University, 1997.

Robertson, Horace B., Jr., ed. The Law of Naval Operations. United States Naval War College International Law Studies, Volume 64. Newport, RI: Naval War College Press, 1991.

Schindler, Dietrich and Jirí Toman, eds. The Laws of Armed Conflicts: A Collection of Conventions, Resolutions and Other Documents, Second Edition. Rockville, MD: Sijthoff & Noordhoff, 1981.

Tzu, Sun. The Art of War. Translated by Samuel B. Griffith. New York: Oxford University Press, 1963.

Yearbook of the United Nations 1974. United Nations: Office of Public Information, 1977.

PERIODICALS:

Dornheim, Michael A. "Bombs Still Beat Bytes." Aviation Week and Space Technology 148, no. 3 (19 January 1998): 60.

Fulghum, David A. "New Weapons Slowed By Secrecy Clampdown." Aviation Week and Space Technology 148, no. 3 (19 January 1998): 54-56.

Harknett, Richard J. "Information Warfare and Deterrence." Parameters XXVI, no. 3 (Autumn 1996): 93-107. Also available from <http://carlisle-www.army.mil/usawc/Parameters/96autumn/harknett.htm>. Internet. Accessed 12 October 1997.

Johnson, Craig L. "Information Warfare – Not a paper War." Journal of Electronic Defense, Vol. 18, No. 8 (August 1994): 55-58.

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War," Parameters XXVI, no. 3 (Autumn 1996): 81-91. Also available from <http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm>. Internet. Accessed 12 October 1997. From the original: Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson. "Strategic Information Warfare: A New face of War" Santa Monica, CA: RAND, 1996. The full text of the study is available from <http://www.rand.org/publications/MR/MR661/MR661.pdf>. Internet. Accessed 12 October 1997.

Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge." Parameters XXVI, no. 4 (Winter 1996-97): 81-91. Also available from <http://carlisle-www.army.mil/usawc/Parameters/96winter/thomas.htm>. Internet. Accessed 12 October 1997.

SPEECHES AND LECTURES:

Cohen, William S. DoD OASD(PA) News Release, reference number 142-97. Remarks as delivered to the Navy League Exposition on 27 March 1997. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

_____. DoD OASD(PA) News Release, reference number 200-97. Remarks as delivered to the Western Hemisphere Symposium on 15 April 1997. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

_____. DoD OASD(PA) News Release, reference number 258-97. Remarks prepared for delivery to the Center for Strategic and International Studies on 22 May 1997. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

_____. DoD OASD(PA) News Briefing. Western Hemisphere Symposium, Crown Plaza Hotel, Miami, Florida on 15 April 1997. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

_____. DoD OASD(PA) News Briefing. Media availability following the Secretary's acceptance of the Bull Simon's Award, McDill AFB, Florida on 16 April 1997. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

_____. DoD OASD(PA) News Briefing. Breakfast meeting, Los Angeles Chamber of Commerce, Loyola Marymount University, Westchester, California on 30 May 1997. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

Johnson, Phillip A., Colonel, USAF. Legal Aspects of Information Warfare. Briefed at the National Defense University School of Information Warfare in January 1997.

White, John. DoD OASD(PA) News Release, reference number 533-95. Remarks prepared for delivery to the Air Force Association Business Session on 15 September 1995. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

_____. DoD OASD(PA) News Release, reference number 264-97. Remarks prepared for delivery to the Chicago Council on Foreign Relations and Mid-America Committee on 22 May 1997. Available from <http://www.defenselink.mil/> with a search for "information warfare." Internet. Accessed on 11 October 1997.

STUDIES AND RESEARCH DOCUMENTS:

Aldrich, Richard W. The Legal Implications of Information Warfare. USAF Institute for National Security Studies Occasional Paper 9. United States Air Force Academy, CO, April 1996.

Computer Emergency Response Team (CERT), Carnegie Mellon University. Available at <http://www.cert.org/>. Internet. Accessed 24 February 1998.

Kuschner, Karl, Major, USAF. "Legal and Practical Constraints on Information Warfare." Available from <http://www.cdsar.af.mil/cc/kuschner.html>. Internet. Accessed 19 December 1997.

Lewis, Brian C. "Information Warfare." Available from <http://www.fas.org/irp/eprint/snyder/infowarfare.htm>. Internet. Accessed 10 October 1997.

Libicki, Martin C. What is Information Warfare? National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology. Washington, D.C.: National Defense University Press, August 1995.

_____. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Second Printing. National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology. Washington, D.C.: National Defense University Press, August 1995.

Minehart, Robert F. "Information Warfare Tutorial." Available from <http://www.fas.org/irp/eprint/snyder/infowarfare.htm>. Internet. Accessed 12 October 1997.

Schwartau, Winn. "Ethical Conundra of Information Warfare." Available from <http://www.infowar.com/mil_c4i/iw_thics.html-ssi>. Internet. Accessed 18 December 1997.

Stein, George J. "Information Attack: Information Warfare in 2025." A research paper presented to Air Force 2025. Available from <http://www.au.af.mil/au/2025/volume3/chap03/v3c3-1.htm>. Internet. Accessed 12 October 1997.

GOVERNMENT PUBLICATIONS:

Clinton, William J. "A National Security Strategy for a New Century." Washington, D.C., May 1997.

Executive Order 12333. "United States Intelligence Activities." 4 December 1981. U.S. Code. Title 50, sec. 401 (1994).

Executive Order 12958. "Classified National Security Information." 17 April 1995. Available from <http://library.whitehouse.gov/Search/Query-ExecutiveOrders.html> with a search for Executive Order Number 12958. Internet. Accessed 6 February 1998.

Executive Order 13010. "Critical Infrastructure Protection." 15 July 1996. As amended by Executive Order 13025 of 13 November 1996, Executive Order 13041 of 3 April 1997, and Executive Order 13064 of 11 October 1997. The text of Executive Order 13010 in its full amended form is available from <http://www.pccip.gov/eo13010.html>. Internet. Accessed 5 February 1998.

Marsh, Robert T. "Critical Foundations: Protecting America's Infrastructures." The Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C., 13 October 1997.

Presidential Approval and Reporting of Covert Actions. U.S. Code. Title 50, sec. 413b (1994).

U.S. Department of the Air Force, Office of the Staff Judge Advocate, Moody AFB. "Legal Aspects of Information Warfare." Available from <http://www.moody.af.mil/wg/ja/ AOR/opsinfo.htm>. Internet. Accessed 19 December 1997.

_____. "Law of Armed Conflict." Available from <http://www.moody.af.mil/wg/ja/AOR/ opsloac.htm>. Internet. Accessed 16 February 1998.

U.S. Department of the Army. Treaties Governing Land Warfare. Pamphlet 27-1. Washington, D.C.: U.S. Department of the Army, 7 December 1956.

_____. The Law of Land Warfare. Field Manual 27-10. Washington, D.C.: U.S. Department of the Army, 18 July 1956 with Change One dated 15 July 1976.

U.S. Department of Defense. DoD Law of War Program. Directive 5100.77. Washington, D.C.: U.S. Department of Defense, 10 July 1979.

_____. Review of Legality of Weapons Under International Law. Instruction 5500.15. Washington, D.C.: U.S. Department of Defense, 16 October 1974.

_____. Compendium of Joint Publications. Joint Publication 1-01.1. Washington, D.C.: U.S. Department of Defense, 25 April 1995.

_____. Joint Doctrine for Information Operations. Joint Publication 3-13, Preliminary Coordination Draft. Washington, D.C.: U.S. Department of Defense, 28 January 1998.

_____. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Joint Staff research report prepared by Science Applications International Corporation. Washington, D.C.: GPO, 4 July 1995.

MEMORANDA:

Rose, Stephen A., Captain, JAGC, USN, Commander in Chief, United States Atlantic Command, Staff Judge Advocate (J02L). "Legal Aspects of Offensive Information Warfare --- Information Memorandum." Memorandum for information warfare game participants. Norfolk, VA, 16 January 1996.

_____. "Legal Aspects of Peacetime Information Warfare --- Command and Control." Memorandum for information warfare wargame participants. Norfolk, VA, 29 January 1996.