INSS OCCASIONAL PAPER 9
Information Warfare Series

The International Legal Implications of Information Warfare

Richard W. Aldrich
April 1996

INSTITUTE FOR NATIONAL SECURITY STUDIES
U.S. Air Force Academy, Colorado

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
01-04-1996

2. REPORT TYPE

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
The International Legal Implications of Information Warfare

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Richard W. Aldrich

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

HQ USAFA/DFES
USAF INSS
2354 Fairchild Dr., Ste 5L27
USAF Academy, CO 80840

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ USAFA/DFES
USAF INSS
2354 Fairchild Dr., Ste 5L27
USAF Academy, CO 80840

HQ USAF/XONP
1480 AF Pentagon, Room 5D518
Washington, DC 20330-1480

10. SPONSOR/MONITOR'S ACRONYM(S)
HQ USAFA/DFES, HQ USAF/XONP

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

A Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Although the definition of information warfare is still evolving, the Air Force has described it as encompassing "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." Because of potential wartime applications, the question arises as to what the legal implications of information warfare are. One initial hurdle posed by the breadth and uniqueness of certain aspects of information warfare is the question of what constitutes an armed attack in the information age.

The Law of Armed Conflict analysis discusses the three basic principles central to LOAC: the principle of military necessity, the principle of humanity, and the principle of chivalry.

Several international treaties may also constrain potential information warfare activities. Most prominent in this area are treaties dealing with outer space. Treaties place limitations on the use of certain satellites to "peaceful purposes." The Treat on Neutral appears to preclude neutrals from interfering with the use of telecommunications lines which cross their countries, which is nearly impossible in many cases.

15. SUBJECT TERMS
Information Warfare, International Law, Cyberwar, USAFA

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UNCLASSIFIED UNLIMITED	33	DR. JAMES M. SMITH
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			**19b. TELEPHONE NUMBER** *(include area code)* 719-333-2717

THE INTERNATIONAL LEGAL IMPLICATIONS OF INFORMATION WARFARE

Richard W. Aldrich

INSS Occasional Paper 9

Information Warfare Series

April 1996

USAF Institute for National Security Studies
US Air Force Academy, Colorado

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense or the US Government. This report is approved for public release by SAF/PAS; distribution is unlimited.

****

ABOUT THE AUTHOR: Richard W. Aldrich is an Air Force Staff Judge Advocate and Associate Professor of Law at the US Air Force Academy. He received a BS in computer science from the Air Force Academy in 1981 and a JD from the UCLA School of Law in 1986.

****

This paper is the result of research conducted under the auspices of an INSS research grant in the summer of 1995.

****

Comments pertaining to this report are invited and should be forwarded to: Director, Institute for National Security Studies, HQ USAFA/DFE, 2354 Fairchild Drive, Suite 5D33, US Air Force Academy, Colorado Springs, CO 80840, 719-472-2717.

TABLE OF CONTENTS

FOREWORD

We are pleased to publish this ninth volume in the *Occasional Paper* series of the US Air Force Institute for National Security Studies (INSS). This monograph represents the results of research conducted during fiscal year 1995 under the sponsorship of a grant from INSS.

This paper examines the international legal implications of information warfare and its basic underlying concepts. As the author points out, we have entered the information age. The US military is the most information dependent force in the world and also the most networked. Add to that the United States' dependence on computers and computer networks for banking, communication, stock exchanges, transportation, air traffic control, and it is obvious that, in the words of the Director of the National Security Agency, "we've become the most vulnerable nation on earth."

Infowar, the ability to destroy or disrupt these networks, has become a major security challenge. Individuals, terrorists, or foreign countries capable of penetrating these infosystems could wreak havoc with our national defense and civilian infrastructures. How does the Law of War and other international law limit this new form of warfare? That question provides the focus for this paper, which raises many issues with no clear legal precedent. In this new arena, the author advocates applying existing law to fill gaps as they are identified, while trying to develop and adapt the law to the changed environment.

About the Institute

INSS is co-sponsored by the National Security Negotiations Division, Plans and Operations Directorate, Headquarters US Air Force (USAF/XOXI) and the Dean of the Faculty, US Air Force Academy. The mission of the

Institute is "to promote national security research for the Department of Defense within the military academic community, and to support the Air Force national security education program." Its primary purpose is to promote research in fields of interest to our organizational sponsors: arms control, proliferation, national security, regional studies, the revolution in military affairs, information warfare, and environmental security. INSS coordinates and focuses outside thinking in various disciplines and across services to develop new ideas for USAF policy making. The Institute develops topics, selects researchers from within the military academic community, and administers sponsored research. We also host conferences and workshops which facilitate the dissemination of information to a wide range of private and government organizations. INSS is in its fourth year of providing valuable, cost-effective research to meet the needs of the Air Staff and our other sponsors.

We appreciate your continued interest in INSS and its research products.

JEFFREY A. LARSEN, Lt Colonel, USAF
Director, Institute for National Security Studies

EXECUTIVE SUMMARY

"Information Warfare" is a fairly new concept. As such, its definition is still evolving, but the Air Force has described it as encompassing "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." The breadth of this definition spans the spectrum from primitive propaganda and deception actions to high tech viruses and morphing techniques. It is a concept which can be employed offensively, defensively, and in peacetime.

Because of potential wartime applications, the question arises as to what the legal implication of information warfare are. This paper focuses only on the international legal implications, analyzing the potential applicability of the Law of Armed Conflict, or the Law of War, and several specific international treaties.

One initial hurdle posed by the breadth and uniqueness of certain aspects of information warfare is the question of what constitutes an armed attack in the information age? The question is important for the purpose of determining what constitutes an unlawful aggressive act allowing for the lawful employment of defensive or counteroffensive force. The answer is less than clear, but appears to revolve around the threat the action poses to a government's authority over its people.

The Law of Armed Conflict analysis discusses the three basic principles central to the LOAC: the principle of military necessity, the principle of humanity, and the principle of chivalry. The principle of military necessity stipulates that targets must have a military goal and be consistent with the laws of war. The principle of humanity deals with proportionality in the

type and degree of force used. The principle of chivalry addresses the use of trickery--both permissible ruses and impermissible perfidy or treachery. None of the principles presents any absolute bar to the use of information warfare concepts, tactics or weapons, though each may limit certain implementations of the concept. Notably, the principle of chivalry may restrict the use of trickery, electronic or otherwise, which abuses a protected status, such as that afforded surrendering troops, Red Cross medical services, and the like.

Several international treaties may also constrain potential information warfare activities. Most prominent in this area are treaties dealing with outer space. Several treaties place limitations on the use of certain satellites to "peaceful purposes," a catch-phrase which has been variously interpreted to mean "non-military" at one end or "nonaggressive" at the other. Additionally, the Treaty on Neutrals appears to preclude neutrals from interfering with the use of telecommunications lines which cross their countries. In an age of packet switching and fiber optic cables, such a task would be nearly impossible in many cases anyway, at least without taking down the neutral's own ability to use its communications equipment.

Information warfare is a concept whose time has already come. The number, type, and scope of information operations seems destined to become more omnipresent. As such it is incumbent that American leaders be cognizant of the existing legal strictures to ensure that such activities conform to the law. This will help preserve the humanity of war and America's moral leadership.

The International Legal Implications of Information Warfare

> *Because exploiting [information systems] will readily cross international borders, we must be cognizant of what the law allows and will not allow. We must have good legal advice as we get into this.*
>
> -- General Ronald R. Fogelman, Chief of Staff, US Air Force[1]

I. Introduction

In the above quote, General Fogelman was speaking of "Information Warfare," the type of warfare believed by many to be the means by which the next "big" war will be fought and more importantly, the means by which future wars will be won. The term itself is enigmatic, embracing concepts as old as war itself and as new as the latest technology. The recent meteoric rise in prominence of the concept is inextricably linked to the dramatic advances in communications technology and information systems, specifically the computer.

> Some scientists suggest that the most important invention is not "wireless communication, flying, the internal combustion engine or the atomic bomb but the digital computer;" for, while the others may be a threat to our environment, our privacy or our lives, none of them can threaten our image of ourselves in the way the computer can.[2]

Nor may any of them affect how future wars are fought as much as the networked digital computer will.

Futurists Alvin and Heidi Toffler, authors of *The Third Wave* and *War and Anti-War*, claim we have entered a new era -- an information age. They

refer to this era as the Third Wave to differentiate it from the agrarian and industrial periods. In the Third Wave, information ascends to become the most important resource and, as such, becomes a significant means of both preventing and/or limiting future wars as well as winning wars.

Many scoff at the idea as so much hype. Perhaps so, but it is important to realize that

> the American military is the most information-dependent force in the world. It uses computers to help design weapons, guide missiles, pay soldiers, manage medical supplies, write memos, control radio networks, train tank crews, mobilize reservists, issue press releases, find spare parts and even suggest tactics to combat commanders.[3]

The American military is also the most networked force in the world, a combination which, absent adequate defenses, makes the American military extremely vulnerable to information attacks. The country's heavy civilian reliance on computers in communications, air traffic control, banking and the stock exchanges, has prompted National Security Agency director, Vice Admiral John McConnell, to comment that, "We're more vulnerable than any nation on earth."[4] The Joint Security Commission has characterized American vulnerability to infowar as "the major security challenge of this decade and possibly the next century."[5] Individuals, terrorist groups or foreign countries capable of penetrating the military's information systems could wreak havoc with our national defense.

Some say the war has already begun. Robert Ayers, of the Defense Information Systems Agency (DISA), has concluded that Department of Defense computers were broken into by unknown persons in excess of 300,000 times in 1994. Indeed, DISA itself tried to test the military's vulnerabilities by hacking into 8,932 DOD computers. DISA successfully gained control of 88% of them, using only "front door" attacks. Even more discouraging is the fact

that only 4% of those hacked into even knew they had been victimized, and shockingly only 0.2% reported it.[6]

How, then, does the law of war and other international law limit this new form of warfare, if at all? To answer that question, this paper will first explore the definition of the term "information warfare," then discuss the appropriateness of applying the laws of war to information warfare techniques. Finally, it will turn to international treaties to determine how they may impact this new form of warfare.

II. Definitions

How the laws of war and international treaties proscribe the scope and use of information warfare hinges largely on how it is defined. Unfortunately, the definitions are diverse. Indeed, there are even various terms used in lieu of or in addition to information warfare including: "infowar," "information operations," "netwar," "command and control counterwar (C^2W)," "Third Wave War," "knowledge war" and "cyberwar."[7]

The term "information-based warfare" is sometimes used to denote a subset of information warfare, but can also describe an earlier, more narrow concept of infowar:

> Information-based warfare is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based warfare is both offensive and defensive in nature--ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets.[8]

Some also distinguish "information age warfare" from information warfare. The former "uses information technology as a tool to *impart* . . . combat operations with unprecedented economies of time and force,"[9] while the latter "views information itself as a separate realm, potent weapon and lucrative target."[10]

"Information assurance" is most often used by non-military individuals and organizations to denote only the defensive aspect of information warfare, though many in the corporate community also employ the term "information warfare" for that purpose.

Winn Schwartau, author of the book *Information Warfare: Chaos on the Electronic Superhighway*, defines information warfare as "an electronic conflict in which information is a strategic asset worthy of conquest or destruction."[11] He also defines three classes of information warfare: Class 1 is personal information warfare, Class 2 is corporate information warfare, and Class 3 is global information warfare.

The Computer Security Institute defines information warfare as,

> [d]istinct from "computer crime" because it implies an aggressive act on the part of one adversary--whether an individual, a competing organization or a rival government--against another in an ongoing struggle for hegemony in the marketplace or the political arena.[12]

It goes on to distinguish the term from "information gathering" by noting that the former carries with it the threat of interrupted operations and destroyed assets in addition to the loss of secrets normally associated with another's information gathering.[13]

According to *The Washington Post*, "The Pentagon formally defines infowar as the effort to seize control of electronic information systems during a conflict."[14] However, this assessment of the Pentagon's definition is far too

narrow. Indeed some in the Pentagon have defined information warfare so broadly that it encompasses virtually all aspects of warfare activity. In a publication recently released by the Air Force, *Cornerstones of Information Warfare*, infowar is defined 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."[15] Under this definition, information warfare is dependent only on the nature of the action, not the means by which it is accomplished. Thus, the conventional bombing of a computer center is information warfare, but would not be under definitions offered by Mr. Schwartau and others.

The National Defense University defines infowar as "the use of information and information systems as weapons in a conflict where information and information systems are the targets." This would presumably include the wartime use of propaganda and psychological operations (PSYOPS).

However the term is defined, its very name may make matters more complicated from a legal perspective. Under the broadest definitions, information warfare could be carried out both during peacetime and in conflict. Calling a peacetime activity "information warfare" may unnecessarily suggest the applicability of the laws of war or the appropriateness of defensive measures. It was perhaps for this reason the United States Army has referred to the concept instead as "information operations." In spite of this, the term "information warfare" seems already too entrenched in the American vocabulary to change anytime soon. And obviously the vocabulary does not drive the law. Calling a pencil a nuclear weapon, for instance, does not make it one, but it would certainly introduce unnecessary confusion if a foreign country learned that the Pentagon was purchasing one million of these new "nuclear weapons."

III. The Law of Armed Conflict

Despite the lack of a universally agreed upon definition, this paper will concentrate on that aspect of information warfare dealing with the use of information systems for offensive or defensive purposes. Conventional attacks against information systems can largely be dealt with using traditional law of armed conflict constructs to assess military necessity, proportionality, collateral damage and the like. It is the use of non-traditional "information weapons" which raises the most interesting legal questions and which will be the focus of this paper.

A. Applicability

1. Armed Conflict

The Law of Armed Conflict is also referred to as the Law of War, though the former term seems more popular as nation states today rarely declare war, but frequently involve themselves in armed conflicts. The Law of Armed Conflict necessarily applies whenever two nation states are involved in an armed conflict.[16] But what is "armed conflict?" The expression "international armed conflict" is not defined in the Geneva Conventions or elsewhere in international law, but several commentators would consider that, at a minimum, it would apply "wherever regular armed forces engage the regular armed forces of a foreign state or enter the territory of a foreign state without permission."[17] "Engage" conveys a physical confrontation, and "enter[ing] the territory of a foreign state" denotes a physical entry, thus in both cases skirting the concerns raised by information attacks. Some may find it less problematic characterizing an information attack as force if there is a physical

manifestation, such as an explosion. But this comprises only a fraction of the potential kinds of information attacks. "Armed conflict," as presently understood, seems far less likely to be applied to the simple manipulation of bits inside a computer, though this may soon change. Already the nefarious manipulation of bits could, in some cases, cause significantly more harm than a bomb.

"Armed conflict" under Article 2 of the Geneva Conventions was specifically chosen over the term "war" because of its broader scope. However, its scope in 1949 could hardly have foreseen today's potential information warfare conflicts. The commentator Jean C. Pictet concluded that, "Any difference arising between two states and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the parties denies the existence of a state of war."[18] This only shifts the question to what constitutes "intervention," but again the defining criteria seems to be one of *physical* confrontation. If an information attack does not fit the definition of an "armed conflict," then many, if not all of the laws of armed conflict are not even applicable.

2. Cyberspace vs. Land, Sea, Air and Space

The Geneva and Hague Conventions both deal with the issues of laws of war "on land" or "at sea." Even the 1977 protocols to update the Geneva Conventions continued this connection to the land or sea, while other law of war treaties dealt with the air and space. This division worked well for the agrarian and industrial ages, but falls far short in proscribing conduct in the information age. Information warfare takes place in what has come to be known as cyberspace, an ethereal place which does not neatly fit into the land, sea, air, space dichotomy.[19] Information warfare involves conduct and effects which transcend national boundaries and render such distinctions superfluous.

Nor do actions in cyberspace come cloaked in military garb. The information attack against a military computer could be the work of a curious teenager down the street, the work of terrorists in a nearby country, or the work of a belligerent government half way around the world. One cannot always trace the source of the action. And even when the action can be traced back, it may lead only to an anonymous remailer. If an ICBM were launched from Russia, it would be a fairly clear signal of the start of an armed conflict. However, even if an information attack could be traced to Russia, it is unclear whether a teen, a terrorist group, or agents of the government are at the keyboard. Some may say that this is no different from the anonymous terrorist attacks occasionally suffered by military personnel and installations. The killing of American soldiers in German discos is a prominent example. In such a case, the United States merely relied on other sources of intelligence to fill in the ambiguities. In the German disco case, intelligence sources were able to sufficiently point the finger at Libya to justify military air strikes against it. Perhaps the same can be done in the area of information attacks, though it is interesting to note that the State Department's Anti-Terrorism unit narrowly defines terrorism to be only politically motivated physical attacks. Thus, information attacks would not generally even fit within the definition of terrorism.

B. Basic Principles

There are three basic principles central to the laws of armed conflict (LOAC) and it is instructive to analyze the applicability of LOAC to information warfare by analyzing these underlying tenets.

1. Principle of Military Necessity

The first principle of LOAC is military necessity. Briefly, it "permits the application of only that degree of regulated force, not otherwise prohibited by the laws of war, required for the partial or complete submission of the enemy with the least expenditure of life, time and physical resources."[20] Professor Francis Leiber defines it as, "Those measures which are indispensable for securing the ends of war and which are lawful according to the modern law and usages of war."[21]

This first principle would seem to pose few hurdles for information warfare. However, the exact scope of term "regulated force" is somewhat nebulous and could pose some problems for the employment of certain types of computer viruses. Viruses are often listed among the available "information weapons" and include worms, Trojan horses and logic bombs. These are all programs or sections of computer code designed to wreak havoc on a recipient's computer. They can be designed to trigger upon the occurrence of a certain event or to activate randomly. Randomly triggered viruses, worms, Trojan horses and logic bombs may not properly fit the definition of the use of *regulated* force.

The Principle of Military Necessity permits anything that is not otherwise prohibited by the laws of war. This definition currently works in the favor of information war advocates, since most of the laws of war were set down prior to any conceptualization of information weaponry and information warfare tactics. While the relative void does little to impede this new form of war, some international treaties may provide barriers.

The stipulation that defeat of the enemy be accomplished with the least expenditure of life, time and physical resources also favors information warfare, since it is largely viewed as a bloodless type of warfare. Information attacks may also take little time, potentially traveling at the speed of light. And because

it is generally aimed at disrupting information systems, information warfare attacks are less likely to result in the loss of physical resources or lives, though some attacks are aimed at destroying internal electronics.

While not much has been published on how information warfare will be conducted, Col Owen E. Jensen recently wrote an article "for those seeking a few fundamental principles to guide them in applying information warfare to specific scenarios."[22] In his article he emphasizes the importance of the Principle of Decapitation:

> Cut or deny *all* the enemy's information-transfer media--telephone, radio frequencies (RF), cable, and other means of transmission. Sever the nervous system. Deny, disrupt, degrade, or destroy *every* transmission. Stop all "gray system" access. Close off to the enemy all third-party communications satellites (COMSAT), whether they belong to international consortia or to commercial enterprises or are assets of uninvolved nations.[23]

The all-inclusive nature of this principle raises several legal issues: (1) its scope probably exceeds the bounds of military necessity, (2) it probably violates the INTELSAT and INMARSAT treaties, and (3) it probably violates the treaty concerning neutrals. Only the first issue will be addressed here. The latter two will be addressed in the appropriate sections below.

Again, the Principle of Military Necessity allows only the application of that degree of regulated force required for the partial or complete submission of the enemy with the least expenditure of life, time and physical resources. Arguably, denying all information-transfer media and disrupting or destroying every transmission goes beyond a military objective by incapacitating the entire civilian populace as well. Taking out all information-transfer media would bring down a country's stock market, banking system, air traffic control, emergency dispatches and more. This would almost certainly result in the loss

of civilian lives, and may well be deemed disproportionate to the military objective. The difficulty in the information age, however, comes in where to draw the line.

In the United States, for example, over 95% of military communications traverse civilian lines. The use of fiber optics and packet switching makes taking out only military communications virtually impossible. Nevertheless, incapacitating the entire civilian system would seem too blunt an approach under the law of armed conflict. Taking out military communications centers, military radio frequencies, and manipulating military messages to create confusion and render even good messages suspect would be a far more legally defensible position. However, if the enemy responded by targeting civilian communications centers and civilian frequencies, a response in kind would be more clearly legal, even with the consequent collateral effects to civilians.

The Air Force's *Cornerstones of Information Warfare* notes a troubling asymmetry between offensive and defensive actions under information warfare:

> The military may, consistent with the law of armed conflict, attack any militarily significant target. In the context of information warfare, this means we may target any of the adversary's information functions that have a bearing on his will or capability to fight. In stark contrast, our military may defend only military information functions. There are many information functions critical to our national security that lie outside the military's defensive purview.[24]

Indeed, as previously noted, over 95% of military communications traffic over commercial communications systems.[25]

The issue raises another point: who is a "combatant" in the information age? If teenage hackers in the enemy's country unilaterally decide to aid their government by creating havoc through their use of computers, do

they become fair game for attack by the opposition? If civilian radio and television stations unwittingly broadcast coded messages to the enemy's troops can they be attacked?

2. Principle of Humanity

The second basic principle is the Principle of Humanity, aimed at prohibiting "the employment of any kind or degree of force not necessary for the purposes of war, that is for the partial or complete submission of the enemy with the least possible expenditure of life, time and physical resources."[26]

The Law of Land Warfare forbade the employment of "arms, projectiles, or material calculated to cause unnecessary suffering." Included as examples were lances with barbed heads, irregularly shaped bullets, bullets with the hard shell heads filed off, bullets dipped in an inflammatory substance, and projectiles filled with glass.[27] The 1981 Convention on the Prohibition or Restriction on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects added weapons which resulted in non-detectable fragments in the body, field mines, booby traps, and incendiary weapons.[28] These proscriptions are all very specific and fail to form any cohesive framework from which logical extensions could be made. Thus, while bullets dipped in an inflammatory substance are banned, the United States has long claimed that nuclear weapons are not *per se* excluded under the principle of humanity. Additionally, all of the specific weapons listed are rudimentary weapons of an older era with little real connection to any of the weapons envisioned for use in information warfare. With such specificity and incongruity it would be difficult to automatically exclude any information weapon, though the overarching ban on weapons calculated to cause unnecessary suffering may provide a hazy boundary.

The theoretical depiction of certain types of computer programs as "weapons" introduces another problem. The law of armed conflict requires any nation desiring to implement a new type of weapon to make a determination, prior to its use, regarding its compliance with the principle of humanity.[29] If a computer program, whether it be a virus, worm, logic bomb or something else, is called a "weapon," this may unwittingly trigger a required review. Certainly computer programs in and of themselves have not previously been considered weapons in the international community, though in some uses their effects may have some striking parallels with conventional weapons.

Some "weapon" use may also be constrained by domestic law even if it is only applied internationally. For instance, if in the course of employing international infowar data collection techniques "United States persons" become subjects, the operation may fall under the purview of Executive Order 12333. The order's applicable provisions are as follows:

> *2.4 Collection Techniques.* Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. . .
>
> *2.5 Attorney General Approval.* The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a

> foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.

While domestic law is beyond the scope of this paper, it is worth emphasizing that even operations taking place entirely in a foreign country or countries may be constrained not only by the foreign country's law and international law, but by domestic law as well. This is not peculiar to information warfare, but applies across the board.

Other data collection techniques will likely be treated in the same way as espionage, that is, while it is not prohibited by the laws of armed conflict, it is punishable by the laws of enemy state if the enemy can capture the spy and exercise its jurisdiction over him or her. Infowar roles which may fit this bill are "sniffing," "dumpster diving," and "cracking."

Sniffing generally entails the use of software to record the first several characters of a telnet session. This information generally includes the username, Internet Protocol (IP) address, and password--enough information for the sniffer to breach security and/or pose as the sniffee.

Dumpster diving, while oftentimes listed as an information warfare technique, is nothing more than the low tech rifling through the opposition's trash in search of userIDs, passwords, and the like to allow infiltration of the enemy's information systems.

Cracking is the more sophisticated use of computers to access or create back doors to the enemy's computer systems. It may also involve setting up Trojan horses, circumventing firewalls, and/or attempting to obtain root access.[30]

In addition to, or in lieu of espionage laws, some countries may also have computer crime laws under which such conduct may be prosecuted. Of particular note is the United Kingdom's Computer Misuse Act. This Act

broadly proscribes many actions which would be included within the sniffing and cracking functions described above:

> (1) A person is guilty of an offence if--
> (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
> (b) the access he intends to secure is unauthorised; and
> (c) he knows at the time when he causes the computer to perform the function that that is the case.[31]

Of even greater significance, however, is the fact that the Act purports to apply extraterritorially, as long as any significant link with British jurisdiction exists.[32] A significant link includes any access of a computer in the U.K.[33] Based on the fact that the Internet is designed to withstand nuclear attack by sending message packets through any working node, the scope of this Act is perhaps broader than would first appear. Thus, if a French operative were to attempt to make a nefarious entry into a U.S. Department of Defense computer and the message, by happenstance were routed through the U.K., the French operative could be tried and convicted under U.K. law. There would, of course, still be the sticky situation of obtaining jurisdiction over the Frenchman. If he were operating under the direction of the French government, France would be unlikely to turn him over. And the Frenchman would be well-advised to vacation somewhere other than England, for fear that upon entering the country authorities there would seize and try him.

3. Principle of Chivalry

The third basic principle of the law of armed conflict is the Principle of Chivalry. Its premise is that the waging of war should be done "in accord with well-recognized formalities and courtesies."[34] This principle recognizes that deception is often key to military victory, and does not outlaw its use, but it

does circumscribe how and when it may be used within the broad constructs of ruses and perfidy (or treachery).

Ruses. By international treaty, "[R]uses of war . . . are considered permissible."[35] Ruses consist of the use of trickery without reliance on any protected sign, symbol or status. The use of misinformation to convince the Iraqis that the United States would attack from the shore was a proper use of a ruse. The ruse was designed to encourage the Iraqis to set up their troops to defend an attack from the shore, thereby allowing for more effective attacks against relatively unprepared forces away from the shore and an unsupported Iraqi rear flank.

Perfidy. Perfidy on the other hand is prohibited under the law of armed conflict. Protocol I to the Geneva Conventions states, "It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy." The protection which one is obliged to accord an enemy is largely identified by certain protected symbols which have been set out in a series of international agreements.

Various treaties have established protected status for symbols designating medical activities,[36] historic, artistic, scientific or cultural objects,[37] civil defense,[38] prisoner of war camps,[39] civilian interment camps,[40] and dangerous forces.[41] The UN emblem, the flags, uniforms and aircraft markings of neutrals and the enemy, and the white flag of surrender[42] all denote a special status.[43]

None of these symbols would seem likely to come into play in information warfare operations. The protected status recognized by these symbols, however, may. For instance, suppose Iraq sent a bogus e-mail

message to low level coalition force commanders in the Gulf purporting to be from the commander of all coalition forces indicating that Iraq has surrendered and all hostilities are to cease immediately. If a commander acted on this message believing it to be real, and suffered heavy casualties from an Iraqi force he thought was surrendering but was actually attacking, would Iraq be guilty of violating the Law of Armed Conflict? The question raised is whether such action constitutes a ruse or perfidy. Arguably, although Iraq did not directly claim to be surrendering, its act of spoofing the United States into so believing and taking advantage of the protected status of surrendering troops, may well place its actions into the category of perfidy and therefore constitute a LOAC violation.

Neutrals. The issue of neutrals may pose interesting legal issues under information warfare. Generally, nation-states desiring to maintain neutrality may not allow belligerents to cross their territory or use their ports except to perform emergency repairs. How then does this general concept apply in the information era where communications channels criss-cross a nation's territory and may well be used by belligerents on either or both sides? The Convention on Neutrals[44] would seem to suggest that a neutral could condone the use of its communications cables without risking its neutrality:

> Art. 8. A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.[45]

However, if a neutral tried to prohibit the use of its communications channels to one of the belligerents it would have to prohibit use of the same to the other belligerent(s) as well or place its neutral status in jeopardy:

> Art. 9. Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents. A neutral Power must see to the same obligation being

> observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus.[46]

In fact, the common use of fiber optic cables and packet-switched networks may well make it nearly impossible to deny the use of communications facilities to a belligerent without also denying those facilities to one's own populace.

Significantly the treaty does not address telecommunications satellites, though the same problems may well exist in selectively denying use to some users without jeopardizing all users.

IV. Treaties

Having reviewed some of the considerations in applying the laws of war to information warfare, this paper will now review the applicability of international treaties and customary international law.[47] The broad definition of information warfare precludes a comprehensive review of all treaties which could have some tangential impact. This section will attempt only to highlight those treaties which would appear to most directly affect the implementation of information warfare operations.

A. The United Nations Charter

The waging of aggressive war was outlawed by Article 2, paragraph 4 of the Charter of the United Nations:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations.

Instead of "war," the Charter used the broader concept of "threat or use of force." While some favored defining aggression in the U.N. Charter, the United States opposed the idea on the grounds that no definition could adequately account for all the circumstances necessary to make such a determination.[48] The United States' position prevailed. This paper does not attempt to refine the definition, but only to provide some insight into the concept's interpretation. The term "force" has sometimes been used in a broad sense to embrace all types of coercion: economic, political and psychological as well as physical. Western nations have largely rejected such a comprehensive definition, the support coming primarily from Third World countries.[49]

The U.N. General Assembly adopted a non-binding definition in its Resolution on the Definition of Aggression.[50] Aggression was limited to the use of "armed force" in Article 1. An enumeration of such acts is set out in Article 3, though Article 4 makes clear the list is not exhaustive.

> The economic, ideological and other modes of aggression were carefully considered . . . but the result was an interpretation that they did not fall within the term 'aggression' as it had been used in the Charter.[51]

Nor did the definition adopted by the General Assembly address the threat of force.

Despite the ambiguity of the terminology used in the Charter and the relatively narrow definition of aggression adopted by the General Assembly, most international attorneys hold that "As long as the act of force . . . compels a State to take a decision it would not otherwise take, Article 2(4) has been violated."[52] This is a very broad interpretation which could potentially pull many information warfare activities within its proscriptive ambit, including propagandizing through the Internet. However, Article 19 of the Universal Declaration of Human Rights declares: "Everyone has the right to freedom of

opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Even if certain actions are clearly identified as unauthorized uses of force, the difficulty then comes in detecting the actions and/or identifying the perpetrator.

> It is not at all clear that information-warfare steps by a potential adversary would be readily detectable: the "How do you know you are at war?" question may be quite difficult to answer.[53]

B. The Outer Space Treaty

The Outer Space Treaty states that "States Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction . . .."[54] The term weapons of mass destruction has generally referred to nuclear, chemical and biological weapons. It is unclear whether the destructive potential of information weapons could move it into this class as well. Even in that event, however, the stipulation that the orbiting object not "carry" such a weapon would seem to militate against the inclusion of information weapons under under a strict reading of this provision. Satellites would act more as a relay point for an information warfare "weapon," than as a "carrier" of the weapon.

The Outer Space Treaty also states that, "The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. . . [T]he testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden."[55] The term "celestial bodies" refers only to natural bodies, such as the moon, asteroids, and planets, not to man-made satellites, and as such would appear to limit little the current scope of information warfare activities. Under this treaty and other space

treaties, states are responsible for insuring that space is used for the benefit of mankind and for peaceful purposes. At least one international legal scholar contends that "This applies to data flows as to any other activity."[56] Indeed the issue of Transborder Data Flow ("TBDF") has become an especially important one in the field of international commerce. The abbreviation TBDF is shorthand for international information transfer, "though TBDF is the more widely used term."[57] What falls within the scope of "peaceful purposes" has met with much debate among international legal scholars, though, "The term 'peaceful' is generally taken to mean nonaggressive as opposed to nonmilitary."[58] Thus, even infowar activities envisioned for the moon or other celestial bodies would apparently not be proscribed by the treaty unless they were aggressive in nature. Even then, some have suggested a non-peaceful purpose may legitimately be made of space objects when acting in "self-defense."[59]

INTELSAT[60] and INMARSAT[61] have similar "peaceful purpose" provisions applicable to classes of satellites. While the same analysis would apply, the likelihood of using these satellites for information warfare operations would presumably be much higher than using the moon or other celestial bodies, so the analysis becomes significantly more important. If a satellite is used to relay military logistical data, is the purpose other than the permitted "peaceful purpose"? Most would probably hold such communications to be routine and not prohibited. What if the same data is relayed in anticipation of war? Would its character then change? Some may argue it does.

C. The Moon Treaty

The Moon Treaty[62] makes reference to the concept of the Common Heritage of Mankind:

> "The Common Heritage of Mankind" ("CHM") is a concept that can be found in the [Moon Treaty], in the United Nations Convention on the Law of the Sea and elsewhere. Broadly, the CHM concept, in part, reflects a belief that all nations should share in an identified resource, even if, in the case of the moon, some nations lack the technological means to access and exploit that resource. At some point a studied attempt probably will be made to apply the CHM concept to information, broadly defined, as a natural resource.[63]

While the term "natural resources" generally conjures images of tangible things, like moon rocks, minerals from asteroids and the like, natural resources can include such intangible natural resources as "the broadcast spectra, orbital positions, and scientific information."[64] Nevertheless, one legal scholar has noted the inappropriateness of applying this doctrine to information, especially when trying to carry with it the rest of the baggage associated with the concept, such as the concepts of sovereignty over resources and depletion of resources.

> Whatever else may be said for the CHM principle, the concept would be difficult to apply to information as a natural resource. It would be illogical and impracticable to attempt to extend a concept such as sovereignty, which has been applied to extraction of mineral resources, to information. Information is not a natural resource.[65]

D. The Liability Convention

Another space treaty also raises issues concerning how information warfare may be impacted by existing international law. Article II of the Liability Convention states that, "A launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight."[66] Based on the fact that the treaty took effect in 1972, it would seem clear that this treaty provision was not intended to constrain the still far-off concept of information warfare. Rather, the provision was likely oriented towards more direct damage, such as that caused by a

falling satellite.[67] The definition of "damage" in Article I does not dissuade one from so concluding, though its language is arguably broad enough to encompass more: "(a) The term 'damage' means loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, national or juridical, or property of international intergovernmental organizations."[68]

Since the treaty does not limit how the space object causes damage, could it be used to assess liability against a state which used a satellite to conduct information warfare operations? It seems unlikely, based on the context in which the treaty was negotiated, but warplanners should at least consider responses to a claim under this provision by a state which claims infowar damages.

Could the term property be construed to include intangible property such as the data stored in a computer? Certainly it could, though again such a reading seems strained. One does not normally speak of "damaged" information, though data which has been corrupted by a virus could be termed damaged.

That the treaty limits liability to damage inflicted "on the surface of the earth or to aircraft in flight," may also raise the issue that it does not extend to data manipulations performed in cyberspace.[69] The counterargument would then be that the collateral damage of the manipulated data occurred on the surface of the earth or to an aircraft in flight.

Art. IV allows for exoneration from liability if the damage to the claimant state (or person represented by the claimant state) was caused by the gross negligence of the claimant or an act or omission done with intent to cause damage. The article goes on to say, however, that there will be no exoneration if the launching state was not complying with international law (specifically the United Nations Charter and the Outer Space Treaty).

While it seems unlikely that this treaty would apply to information warfare, a contrary determination could prove exceptionally expensive.

> The compensation which the launching State shall be liable to pay for damage under this Convention shall be determined in accordance with international law and the principles of justice and equity, [to return the claimant to the *status quo ante*.][70]

Some recent novels and conjecture in the popular press have suggested the possibility of a nation taking out Wall Street or the Federal Reserve system.[71] Consider the costs of returning the United States to the *status quo ante* after such a debacle.

E. The International Telecommunication Convention

The International Telecommunication Convention may further constrain the information war planner. It states that, "All stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members . . ."[72] *Time* magazine reported that "the Air Force's latest secret weapon" is a converted cargo plane named Commando Solo.[73] Commando Solo can purportedly "jam a country's TV and radio broadcasts and substitute messages--true or false--on any frequency." This would appear to be a violation of both the above cited article and Art. 37, which reads, "Members agree to take the steps required to prevent the transmission or circulation of false or deceptive distress, urgency, safety or identification signals . . ."[74] But Art. 38 of the same treaty states, "Members retain their entire freedom with regard to military radio installations of their army, naval and air forces."[75]

F. Guidelines for the Security of Information Systems

The Organisation for Economic Co-operation and Development (OECD) on November 26, 1992, adopted guidelines for the security of information systems.[76] The OECD comprises 24 countries in North America, Europe and the Pacific region. The Group of Experts which prepared the document consisted of government delegates and scholars in various fields including law and computer science. Indeed the Group of Experts was chaired by an attorney, the Honorable Michael Kirby, President of the Court of Appeal, Supreme Court of New South Wales, Australia. Unfortunately, the Guidelines sidestep the issue of information warfare, never mentioning it under any of its various rubrics throughout the document. The Guidelines do address computer crime, and to this extent address some of the same concerns raised by information warfare. Though, in the end the Guidelines are just that, guidelines.

The Guidelines also address the problem of jurisdictional competence, suggesting that countries seek to harmonize their rules on extraterritorial jurisdiction and review their domestic law to determine its suitability for dealing with transborder offenses.[77] In addition, the Guidelines encourage the adoption of international agreements. In the meantime, however, the Guidelines make clear the they "do not affect the sovereign rights of national governments in respect of national security and public order ("ordre public"), subject always to the requirements of national law."

V. Conclusion

General Fogelman was insightful for recognizing the importance of ascertaining the legal boundaries and implications of activities taking place

under the catch phrase of information warfare. Unfortunately, for the same reasons that many recognize this information age as a Third Wave or new era, many of the issues now being raised are without clear precedent.

This paper dealt only with the international legal implications, and in this arena we see that most of the treaties and customary international law to which legal scholars are looking for guidance was developed, in many cases, decades before information warfare concepts were envisioned. Nevertheless, certain basic principles can be carried forward--principles such as military necessity, proportionality and chivalry. The specifics in how these general principles will be applied to certain information warfare scenarios will likely require gradual honing. As countries begin to agree on certain standards, these may well develop into a new customary international law. More immediate desires for regulatory guidance may prompt nations to seek consensus through the treaty making process.

Some prominent thinkers have claimed that our First and Second Wave legal system is so hopelessly unable to deal with Third Wave issues, that it must be replaced promptly, and ignored to the extent necessary in the interim. This seems an overreaction prone to anarchy. On the other hand, some claim that the issues raised by information warfare are really no different than those that have been raised throughout time and that thoughtful application of the existing law is all that is needed. This extreme also seems off the mark and betrays a naïveté of dealing with complex issues in an entirely new realm. 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. The fast moving world of the Third Wave will provide challenges in accomplishing this, but the ease and speed with which information can be exchanged may also facilitate the task.

ENDNOTES

[1] *Computer World*, June 5, 1995, p. 5

[2] Manfred Lachs, *Article: Views From The Bench: Thoughts On Science, Technology And World Law*, 86 A.J.I.L. 673 (1992) (Judge and former President of the International Court of Justice) citing Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation* (1976).

[3] *Washington Post*, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," July 16, 1996, p. C03.

[4] *Time*, "Onward Cyber Soldiers," Aug. 21, 1995, p. 44.

[5] *Time*, "Onward Cyber Soldiers," Aug. 21, 1995, p. 40

[6] *Washington Post*, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," July 16, 1996, p. C03.

[7] John Arquilla and David Ronfeldt, of The RAND Corporation, have defined information warfare as being the sum of netwar and cyberwar. Netwar they define as "societal-level conflict waged through Internetted modes of communication." Cyberwar they define as "conducting and preparing to conduct military operations according to information principles."

[8] Working definition recognized by the School of Information Warfare and Strategy of the National Defense University as of 11/16/93.

[9] Department of the Air Force, *Cornerstones of Information Warfare*, at 2 (1995).

[10] *Cornerstones of Information Warfare*, at 3.

[11] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, p. 13 (1994).

[12] Richard Power, *Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare*, p. 27 (1995).

[13] *Ibid.*

[14] *Washington Post*, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," July 16, 1996 at C03.

[15] *Cornerstones of Information Warfare*, at 3. This definition is similar to one proposed by the Office of the Assistant Secretary of Defense for C^3I.

[16] The Law of Armed Conflict also applies to certain conflicts internal to a nation-state, but that is beyond the scope of this paper.

[17] Lieutenant Colonel William J. Fenrick, *Article: The Rule Of Proportionality And Protocol I In Conventional Warfare*, 98 Mil. L. Rev. 91 (1982) [Lt Col Fenrick was a Legal Officer with the Canadian Forces.]

[18] The Geneva Conventions of 12 August 1949, Commentary 20 (1958).

[19] The legal ambiguities raised by cyberspace are not unique to discussions of information warfare. Computer crimes have raised some of the same issues. To what extent can Muslim countries enforce their criminal sanctions against the importation of pictures of scantily clad women when Internet sites around the world offer such pictures to anyone with a modem or other means of accessing the Internet. Or take the example of offering unauthorized gambling nationwide. One Internet site in Turks and Caicos is already doing so, despite the objections of the U.S. Department of Justice. So far the Justice Department has been unable to prevent the gambling outfit from continuing its operations.

An attack on the military's Rome laboratories in New York by a British hacker resulted in a conviction primarily because both the United States and Britain had laws outlawing the particular conduct engaged in by the hacker and agreed to cooperate in the capture and prosecution of the individual. Adept hackers oftentimes travel electronically through several countries en route to the target of their attack, both to befuddle the investigator and to complicate the international legal issues involved in their arrest and prosecution.

[20] The Air Force Judge Advocate General School, *The Military Commander and the Law 580*, (September 1994).

[21] General Orders 100, Section I, paragraph 14.

[22] Col Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal* (Winter 1994).

[23] *Ibid.* at 37 (emphasis added).

[24] *Cornerstones of Information Warfare*, at 3 n.1.

[25] Science Applications International Corporation, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, A Research Report for the Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington, DC (July 4, 1995). The fact that a country's military uses civilian

communications for a large portion of its message traffic increases the justification for claiming such a target is a military target.

[26] *The Military Commander and the Law* 580 (September 1994).

[27] Article 34, Field Manual 27-10 (1956).

[28] Some may claim the Convention did not "add" these weapons to the list of forbidden weapons, but reduced to writing that which, over time, had already come to be recognized by many countries around the world.

[29] Protocol I to the Geneva Conventions, Art. 36. Indeed, a new "means or method" of warfare requires a similar determination under the article: "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 some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."

[30] Firewalls are computers which serve as protective front-ends to a network. All traffic which seeks access to the network must pass through the firewall computer, which is designed to ferret out intruders. Root access is that access level which allows the user to execute the widest range of commands. Such access is normally only afforded to the system operator. Hackers who obtain such access can wreak havoc on the system.

[31] Section 1(1), *Computer Misuse Act 1990*.

[32] Section 4(2), *Computer Misuse Act 1990*.

[33] Section 5(2), *Computer Misuse Act 1990* reads:

> (2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction--
>
> (a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function; or
>
> (b) that any computer containing any program or data to which the accused secured or intended to secure unathorised access by doing that act was in the home country concerned at that time.

[34] *The Military Commander and the Law* 581 (September 1994).

[35] *The Hague Regulations of 1907*, Art. 24.

[36] Red Cross, Red Crescent, Red Lion and Sun, or Red Star of David. (Art. 38, 1949 Geneva Convention I and Art. 18, 1977 Geneva Protocol I, to the 1949 Geneva Conventions. The Red Lion and Sun is largely obsolete since on September 4, 1980 Iran indicated its intent to use the Red Crescent henceforth).

[37] Red circle with triple red spheres in the circle on a white background (Roerich Pact of 1935) or royal blue square and triangle on a white shield (Art. 16, 1954 Hague Convention and Art. 20, The Hague Regulations) or rectangular panel divided diagonally into two triangular portions, the upper black and the lower white (Art. 5, 1907 Hague Convention IX).

[38] Blue triangle on orange background (Art. 66, 1977 Geneva Protocol I, to the 1949 Geneva Conventions).

[39] PW or PG on a square flag (Art. 23, 1977 Geneva Protocol I, to the 1949 Geneva Conventions).

[40] IC on a square flag (Art. 83, 1977 Geneva Protocol I, to the 1949 Geneva Conventions).

[41] Three bright orange circles of equal size on the same axis (Art. 56(7), 1977 Geneva Protocol I, to the 1949 Geneva Conventions).

[42] White flag is recognized as a symbol of surrender under Article 32, 1907 Hague Regulations.

[43] *Air Force Pamphlet 110-34*, 25 July 1980.

[44] *Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land,* The Hague, October 18, 1907.

[45] *Convention on Neutrals.*

[46] *Convention on Neutrals.*

[47] The applicability of some of the treaties discussed *infra* was raised in an unpublished "Legal Roadmap" document prepared in 1993 by the Aegis Research Corp.

[48] Whiteman, *Digest of International Law* 740, (1965).

[49] Schachter, *International Law in Theory and Practice* 110-113 (1991).

[50] G.A. Res. 3314 (XXIX) (1974), G.A.O.R. 29th Sess., Supp. 31 at 42.

[51] Broms, *The Definition of Aggression*, 154 Rec. des Cous 299, 386 (1977-I).

[52] Schacter, *International Law in Theory and Practice* 110-113 (1991). Many international attorneys find support for their belief in the International Court of Justice cases involving the Corfu Channel and Nicaragua.

[53] George F. Kraus, Jr., CDR (ret.), U.S. Navy, "Information Warfare in 2015," *Proceedings* p. 42 (Aug. 1995)

[54] Article IV of the Treaty on Principles Governing the Activities of States in the Exploitation and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 UST 2410, 610 UNTS 205 [hereinafter the Outer Space Treaty]. The United States is a signatory to this treaty, as are Australia, Bulgaria, Canada, Czechoslovakia, Denmark, Finland, the German Democratic Republic, Hungary, Japan, Mongolia, Nepal, Niger, Republic of Korea, Sierra Leone, Sweden, Ukrainian Soviet Socialist Republic, Union of Soviet Socialist Republics, United Arab Republic, and Great Britain.

[55] Article IV of the Outer Space Treaty. Similar language is included in the Treaty Governing the Activities in Outer Space, on the Moon, and Other Celestial Bodies, G.A. Res. 34/68, 34 U.N. GAOR Supp. (No. 46) at 77, U.N. Doc. A34/46 (1979) [hereinafter Moon Treaty].

[56] Ronald Wellington Brown, "Perspective: Economic and Trade Related Aspects of Transborder Data Flow: Elements of a Code for Transnational Commerce," 6 *J. Intl. L. Bus.* 1, 1 (Spring 1984) (footnotes omitted).

[57] Brown, at 2.

[58] Pamela L. Meredith, "The Legality Of A High-Technology Missile Defense System: The ABM And Outer Space Treaties," 78 *A.J.I.L.* 418 (1984) citing S. Gorove, *Studies in Space Law: Its Challenges and Prospects* p. 85-94 (1977); S.H. Lay & H. Taubenfeld, *The Law Relating to Activities of Man in Space* p. 25 et seq. (1970); D. Goedhuis, *The Changing Legal Regime of Air and Outer Space* p. 27 (1978); N. Matte, *Space Policies Program Today and Tomorrow* p. 68 (1980). She notes also that some scholars are of a different opinion, specifically referencing Lachs and Vlasic.

[59] See Andrzej Jacewicz and Jerzy Markowski, Kosmos A. Zbrojenia, *Aspekty Polityczne, Militarne, Prawne* [Outer Space and the Arms Race. Political, Military and Legal Aspects].

[60] *Agreement Relating to the International Telecommunications Satellite Organization*, p. 23 UST 3813, TIAS No. 7532 (Aug. 20, 1971) [hereinafter cited as INTELSAT Agreement].

[61] *Convention on the International Maritime Satellite Organization*, p. 31 UST 1, TIAS No. 9603 (Sept. 3, 1976) [hereinafter cited as INMARSAT].

[62] *The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, 18 I.L.M. 1434 (1979), has not been ratified by the United States.

[63] Brown, pp. 65-66.

[64] Brown.

[65] Brown, p. 68.

[66] *Convention on International Liability for Damage Caused by Space Objects* [hereinafter the Liability Convention], 24 UST 2389, TIAS No. 7762, reproduced in 10 ILM 965 (1971). The Convention on Registration of Objects Launched Into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, T.I.A.S. No. 8480, 1023 U.N.T.S. 15 [hereinafter Registration Convention], appears to provide assistance for those seeking compensation. It requires all launching states to register their space objects, thus making it easier to assign liability when the infliction of damage can be associated with a registered object:

In order to promote international cooperation in the peaceful exploration and use of outer space, States Parties to the Treaty conducting activities in outer space . . . agree to inform the Secretary-General of the United Nations as well as the public and the international scientific community, to the greatest extent possible and practicable of the nature, conduct, locations and results of such activities. On receiving the said information, the Secretary-General of the United Nations should be prepared to disseminate it immediately and effectively. (Art. XI.)

[67] A later reference to component parts may further this interpretation: "Each State Party to the Treaty that launches or procures the launching of an object into outer space . . . is internationally liable for damages to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth . . .." (Art. VII)

[68] Art. I, Liability Convention.

[69] Art. III allows for liability for damage "caused elsewhere than on the surface of the Earth," but extends it only to damage caused to space objects or person or property on board such space objects.

[70] Art. XII, Liability Convention.

[71] See, e.g., Tom Clancy, *Debt of Honor; Time*,"Onward Cyber Soldiers," Aug. 21, 1995 p.43, and others.

[72] Art. 35, *International Telecommunication Convention*, Malaga-Torremolinos, Oct. 25, 1973, 28 UST 2495, TIAS No. 8572. The Law of the Sea Treaty has a similar provision, there prohibiting the broadcasting from the high seas so as to interfere with the radio broadcasts of coastal states.

[73] *Time*, "Onward Cyber Soldiers," Aug. 21, 1995 at 43.

[74] Art. 37, *International Telecommunication Convention*.

[75] Art. 38, *International Telecommunication Convention*. Paragraph 2 of Art. 38 states: "Nevertheless, these installations must, so far as possible, observe statutory provisions relative to giving assistance in case of distress and to the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed." It would seem that jamming all of a country's stations and substituting for them the transmissions of a belligerent would constitute a "harmful interference." The language "so far as possible" which precedes this section may afford the squirm room necessary to circumvent this provision in time of conflict.

[76] OCDE/GD (92) 190, Paris 1992.

[77] OCDE/GD (92) 190, at 33.

INSS OCCASIONAL PAPERS

1. ***Explaining Weapons Proliferation: Going Beyond the Security Dilemma.*** Gregory J. Rattray, July 1994

2. ***The Ukrainian Military: Instrument for Defense or Domestic Challenge?*** Oleg Strekal, November 1994

3. ***North Korea's Nuclear Program: The Clinton Administration's Response.*** William E. Berry, Jr., March 1995

4. ***Environmental Assistance as National Security Policy: Helping the Former Soviet Union Find Solutions to its Environmental Problems.*** Robert L. Dunaway, November 1995

5. ***Economic Power in the Sino-U.S. Relationship.*** Kevin F. Donovan, December 1995

6. ***Nuclear Proliferation: Diminishing Threat?*** William H. Kincade, December 1995

7. ***Nuclear Proliferation: The Diplomatic Role of Non-Weaponized Programs.*** Rosalind R. Reynolds, January 1996

8. ***Five Minutes Past Midnight: The Clear and Present Danger of Nuclear Weapons Grade Fissile Materials.*** Guy B. Roberts, February 1996

UNITED STATES AIR FORCE ACADEMY

Lieutenant General Paul E. Stein
Superintendent

Brigadier General Ruben A. Cubero
Dean of the Faculty

HEADQUARTERS, US AIR FORCE
PLANS AND OPERATIONS DIRECTORATE

Major General Robert E. Linhard
Director of Plans

Lieutenant Colonel Todd Bodenhammer
Chief, National Security Negotiations Division

USAF INSTITUTE FOR NATIONAL SECURITY STUDIES

Lieutenant Colonel Jeffrey A. Larsen
Director

Major Timothy J. Krein
Editor

Ms Marsha Taylor
Cover Design

USAF Institute For National Security Studies

USAFA/DFE
2354 Fairchild Drive, Suite 4K25
US Air Force Academy
Colorado Springs, CO 80840

(719) 472-2717
DSN: 259-2717
FAX: (719) 472-2716