NAVAL WAR COLLEGE
Newport, RI

COMPUTER NETWORK ATTACK AS A TOOL FOR THE OPERATIONAL COMMANDER

by

T .V. Smits
Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College of the Department of the Navy.

Signature: T .V. Smits

8 February 2000

Jonathan P. Edwards
Faculty Advisor
Jonathan P. Edwards
Captain, JAGC, U.S. Navy

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): COMPUTER NETWORK ATTACK AS A TOOL FOR THE OPERATIONAL COMMANDER (U)	
9. Personal Authors: Theodore V. Smits, LCDR USN	
10.Type of Report: FINAL	**11. Date of Report:** 8 Feb 2000
12.Page Count: 27	**12A Paper Advisor (if any): Jonathan P. Edwards, CAPT, JAGC, USN**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:

Information Warfare, Computer network warfare, Law of War, Law of Armed Conflict, proportionality, humanity, Protocol 1, international law, necessity, chivalry.

15.Abstract: Computer network attack provides the capability for an attack to be carried out at the speed of light, effortlessly across international boundaries. It has the potential to provide the Operational Commander additional capabilities along the entire spectrum of warfare from deterrence to combat operations. Key enemy systems, including radar, air traffic control and communications have the potential to be rapidly removed from operation without having to move a single plane, put U.S. personnel in harms way or expend expensive precision guided munitions. However, the law of armed conflict and other international laws raise legal issues that potentially limit the implementation of this new weapon. The Operational Commander must be knowledgeable of the basis of the legal issues so that suitable network attack targets can be selected during the operational plan development, targets against which an attack plan can be developed and approved in the period required to support the attack's employment in the conflict.

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED	
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT	
19.Telephone: 841-6461	**20.Office Symbol:** C

Security Classification of This Page Unclassified

TABLE OF CONTENTS

COMPUTER NETWORK ATTACK AS A TOOL FOR THE OPERATIONAL COMMANDER

ABSTRACT

Computer network attack provides the capability for an attack to be carried out at the speed of light, effortlessly across international boundaries. It has the potential to provide the Operational Commander additional capabilities along the entire spectrum of warfare from deterrence to combat operations. Key enemy systems, including radar, air traffic control and communications have the potential to be rapidly removed from operation without having to move a single plane, put U.S. personnel in harms way or expend expensive precision guided munitions. However, the law of armed conflict and other international laws raise legal issues that potentially limit the implementation of this new weapon. The Operational Commander must be knowledgeable of the basis of the legal issues so that suitable network attack targets can be selected during the operational plan development, targets against which an attack plan can be developed and approved in the time period required to support the attack's employment in the conflict.

I. INTRODUCTION

Military weapons and strategy reflect the politics, economy and, perhaps most importantly, the technology of a given society. Hence, it is not surprising the improvements in computers, communications, and other electronic data processing systems that are changing society are also changing military thinking and planning.[1] The genesis for this change is that virtually every industry and civil infrastructure has integrated inexpensive, extremely capable data processing systems and computer networks into its organizations in an effort to improve product quality or production efficiency. This integration, while increasing efficiency and productivity, has created dependencies on computer networks that did not historically exist. In many instances, integration of computers and networks has become so complete that failure or disruption of a system causes entire processes to come to a grinding halt. An example of this was demonstrated during a 1997 exercise called Eligible Receiver. During this evolution, hackers from the National Security Agency proved they could cause power outages and 911 emergency system overloads in a number of cities, gain "supervisory" access to military networks, and disrupt e-mail and phone traffic.[2]

The above exercise demonstrates the U.S. had the capability for computer network warfare years ago, yet it has failed to materialize as a viable tool for the Operational Commander. This paper argues that legal issues resulting from the application of the law of armed conflict and other international law are the primary rationale behind the lack of network attack capability. While there is little the Operational Commander can do to alter a network attack's legal review process, understanding the basis of the legal issues can be of significant benefit. With this knowledge, the Operational Commander can provide direction for network

attack target selection which minimizes potential legal issues and therefore maximizes the potential for an attack to be approved and ready to implement when required.

II. INFORMATION WARFARE

The media has an inexhaustible reservoir of labels to describe the concept of computers as a warfare weapon. Since each one means different things to different people, some clarification is required before going too much further. A good working definition of Information Warfare (IW) is provided by the Air Force as: any action to deny, exploit, corrupt or destroy the enemy's information and its functions while protecting assets against those actions and exploiting its own military operations.[3] A simplified version of this is: disrupt the enemy's information or information flow while protecting your own. In order to better understand what IW encompasses, it can be broken into four basic categories: intelligence (gathering of electronic information), offensive computer weaponry (modifying internal software or hardware to cause the enemy's computer to behave other than expected), directed energy type weaponry (such as electro-magnetic pulse weapons), and psychological operations (propaganda, computer enhanced misinformation).[4] While all categories of IW are important to the Operational Commander, the focus herein has been narrowed to offensive computer weaponry, specifically the use of computer network attacks as a weapon during conflict.

The establishment of a computer network defense mission for U.S. Space Command in 1999 is indicative of the priority the U.S. has placed on protecting its systems. While the U.S. Military has practiced defensive actions at various levels for years, this new mission will create a single source of network defense expertise and direction. And recently, to compliment the computer network defensive mission, the military has announced an offensive stance in an effort

to exploit the vulnerabilities of potential enemies.[5] The mission of computer attack has been formally assigned to the U.S. Space Command beginning October 2000. This new mission will include helping U.S. commands around the world in information warfare attacks with the goal of disrupting and degrading enemy systems. However, as the concept of offensive network warfare becomes institutionalized, many legal questions are being raised. The issues are a result of applying the Law of Armed Conflict (LOAC) and other international law to encompass a weapon whose delivery mechanism and capabilities were not conceived when the laws were developed.

The legal issues that arise from network warfare during conflict are centered around a number of areas. These include the definition of an armed attack when applied to a computer attack, the selection of potential targets and their evaluation against the LOAC, and aspects of neutrality, sovereignty and foreign national law. Similar problems surface when applying the concept of network attack during peacetime, or the non-hostility phase of a conflict. Regardless of the phase, few parallels can be drawn to standard kinetic weapons and procedures currently in practice.

III. NETWORK WARFARE AND INTERNATIONAL LAW

A. PRE-HOSTILITIES

Prior to force being used, a wide variety of actions are typically implemented in an effort to coerce or deter a belligerent state. These actions, known as flexible deterrent options,[6] range from economic sanctions to diplomatic initiatives. They provide the Operational Commander considerable latitude without resorting to the use of force. The addition of network attack could

provide an additional set of alternatives to help deter a particular nation. One could envision an information sanction similar to an economic sanction or the generation of civil unrest against the current government by disrupting infrastructure services.[7] However, use of these actions during non-hostility operations bring up issues that include: What is an armed attack? At what point does it become an armed attack and violate the United Nations Charter prohibition on the use of force?[8] What will be the world opinion to information operations during non-hostility periods?

An answer to the first question is readily available; an armed attack in the information world is generally defined as data manipulation that results in destructive effects that are indistinguishable from those caused by traditional (kinetic) weapons.[9] The second question is more difficult since there is very little guidance on small, low level network attacks. However, many believe these lower scale attacks will be judged by the international community by their results.[10] For example, an attack that causes disruption to an administrative database would be difficult to be labeled as an armed attack. But one that disrupted a nation's air traffic control, or significant portions of a power distribution system, and resulted in civilian deaths would probably be determined an armed attack.

On the other end of the spectrum, there are some that feel any implementation of computer attacks during peacetime as deterrence or as part of a plan to affect decisions of a rogue state may be viewed as terrorism by the international community.[11] This unknown reaction by the international community and lack of any legal guidance for implementing various levels of attack have the potential to negatively bias the pre-hostility network attack decision process. The bias could cause delays in the approval process, curtail the severity (effectiveness) of attacks, or perhaps prohibit them altogether.

B. THE USE OF FORCE

The United Nations Charter is the primary international document which provides circumstances when the use of force is authorized. Articles 39 (United Nations sanctioned) and 51 (self defense) state respectively:

> "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be take...to maintain or restore international peace and security." [12]
>
> and
>
> "Nothing in the present Charter shall impair the inherent right of individual or collective self defense if an armed attack occurs against a member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." [13]

When force is deemed necessary and authorized, it must follow a collection of international laws, customs and treaties commonly referred to as the Law of Armed Conflict (LOAC).[14] The LOAC serves to limit destructiveness during war by protecting noncombatants and their property, providing humane treatment or prisoners and limiting the types of weapons that can be used against an enemy. It is generally broken down into four main principles: military necessity, humanity, proportionality and chivalry, which are summarized below:

- Military necessity: The essence of this concept is that capability for destruction does not translate into authorization for destruction. Military personnel/equipment and civilian personnel/property that make a direct contribution to the war effort may be attacked. However, deliberately applying more force than what is required to achieve this objective, such as trying to kill surrendering enemy combatants, is a violation.

- Humanity: This concept seeks to prohibit unnecessary suffering by prohibiting indiscriminate weapons which do not differentiate between military and civilian personnel and property. One of the many treaties and laws that make up the LOAC that is particularly relevant to humanity is the Protocol I Additional to the Geneva Convention. It refines the humanitarian concept and provides specific rules for the protection of noncombatant civilians.[15] Although the U.S. has never ratified Protocol I, it is generally recognized that most of the articles dealing with the protection of the civilian population deserve treatment as customary international law. [16]

- Proportionality: This principle attempts to ensure the ends justify the means. It states that attacks may be carried out against lawful military targets even if some collateral damage and incidental injury is foreseeable as long as the damage is not disproportionate to the military advantage of the target. Proportionality gives the Commander the responsibility to determine if incidental injuries and collateral damage are excessive based on a reasonable assessment of the facts available at the time of the attack. Another significant aspect of this rule is that the defender has the responsibility to separate troops and equipment from noncombatants and civilian property.

- Chivalry: Chivalry provides for war to be carried out with recognized rules and courtesies. For example, with few exceptions, only members of a nation's armed forces can use force against an enemy. They must distinguish themselves from noncombatants and cannot use noncombatants or civilian property as a shield. It also establishes that perfidy, or faking surrender, is not legal and that use of certain visual and electronic symbols identifying persons/property exempt from attack, such as wounded and sick and medical personnel, vehicles and vessels is also prohibited.

IV. APPLICATION OF THE LAW OF ARMED CONFLICT TO NETWORK ATTACK

An implication of network attack is that the attacker probably will not be physically present where the effects of the attack are being felt. Additionally, the means of attack may not be present either. These aspects will complicate the application of the LOAC, which was developed in response to territorial invasions and kinetic weapons the victim could see, and whose source was readily apparent.[17]

The application of the concept of necessity for a network attack is very similar to its application for a kinetic weapon attack. When force is authorized, military networks are obviously lawful targets. However, in order to attack civilian systems there must be a definite military advantage, or necessity, realized from the attack. For example, during conflicts which last only months, it would be difficult to justify attacking economic and production centers, which have little effect on a short duration conflict. The same targeting analysis must be performed for network attacks as for kinetic weapon attacks.[18]

Proportionality presents one of the more significant challenges to information warfare. The coupling of incredible destructiveness with virtually no physical damage raises questions as to what will be accepted as "proportional" in the eyes of the international community. Infrastructure and communication systems, such as emergency medical, police and fire are becoming increasingly interdependent. The unknown interdependence of these systems and potential cascading effects into other, unforeseen areas introduce uncertainties into the network attack damage estimation process.[19] The uncertainties make estimations by the Commander regarding proportionality extremely difficult. One concept to counter this uncertainty is to stage "mini" network attacks to quantify the network vulnerabilities before staging a debilitating attack. Although this may be feasible in some circumstances, the difficulties in staging a small-

scale attack with similar characteristics, coupled with the difficulties of assessing impact and damage of the "mini" attack, will rarely make this a viable option. Additionally, a mini attack may alert the enemy to your intentions and make them aware of their vulnerabilities.

When carrying out network attacks, the rule of humanity poses problems similar to those posed by proportionality which are the unforeseen consequences resulting from the unknown interdependence of systems. For example, an enemy air control system may be the target of a network attack. But, if that air control system is linked with a civilian air control system, numerous civilians could be at risk, and the international community would not view the attack favorably.

Protocol I to the Geneva Convention contains many provisions applicable to a network attack which must be complied with regarding the protection of civilians and which potentially restrict the method and target selection of an attack.[20] One of the more relevant provisions, which provides protection against indiscriminate attack, is found in article 51(4) which states:

> Indiscriminate attacks are prohibited. Indiscriminate attacks are:
> (a) those which are not directed at a specific military objective;
> (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or
> (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol.[21]

Additionally, part of article 57 2 (b) requires an attack to be canceled or suspended if it becomes apparent the object is not a military one.[22] The criteria could cause constraints to be imposed on the type of attacks available. The commercial sector has shown that computer viruses are extremely "indiscriminate" in the way they propagate and would be difficult, if not impossible, to cancel or recall once initiated.

The concept of chivalry serves to protect civilian and other noncombatant personnel, such as those attending the sick and wounded. It was developed when enemies could see each other and clothing (uniforms), vehicle and vessel markings were used as distinguishing features from noncombatants. Although the long distance potential of network attacks makes the wearing of uniforms of little importance, chivalry places restraints on the Commander when carrying out an attack. The LOAC requires combatants be trained in the law of war, serve under effective discipline, and be under the command of officers responsible for their conduct. The DoD Office of the General Counsel concluded that these elements of the LOAC require information warfare operations be conducted only by uniformed forces.[23] Since significant expertise is required to implement an information attack and active duty forces are constantly shrinking, particularly those with information technology expertise, this rule will be challenging to meet.

Other aspects of chivalry that must be carefully evaluated are ruses and misinformation. As information warfare makes these acceptable tactics increasing easier to implement, each must be individually evaluated. A "misinformation" attack such as changing the enemy's database to show U.S. troops are a hospital base or neutral county forces is clearly a violation. However, the LOAC implications concerning other subtle attacks, such as changing enemy databases so that attacking forces electronically appear to be friendly forces are very nebulous.[24] This particular type of network attack could arguably be viewed under the prohibition of attacking while wearing enemy uniforms.

V. OTHER INTERNATIONAL LAWS, TREATIES AND CHARTERS

The ability of electronic signals, which have the potential to represent an armed attack, to cross international boundaries, presents significant challenges regarding sovereignty and

neutrality. Sovereignty has been a fundamental part of international law since the Treaty of Westphalia of 1648. It provides that nations have exclusive authority over all events within their borders. The situation network attack brings to the table is utilization of communication lines. While a nation may have agreed to international communication connections, the transformation of their communications system into a delivery vehicle for an armed attack by an outside state is a significant infringement of their sovereignty.

Closely coupled with sovereignty is the right of neutrality of a State. The Hague Convention determined the territory of a neutral state is inviolable.[25] This implies that using a neutral country's networks or communication lines as a transport path to carry out a network attack would violate the country's neutrality rights similar to aircraft flying over a neutral country's airspace. Using the Hague convention as a basis, proponents argue that a neutral power is not required to restrict the use on behalf of the belligerents of telephone cables or of wireless telegraphy equipment belonging to it or to companies.[26] The difficulty with this argument is that the Hague Convention was convened in 1907. At that time telegraphy equipment only enhanced communications and it was not conceived that telephone lines could be the delivery vehicle (or pathway) of an armed attack. A modern application could interpret the usage of a neutral country's communication lines as a violation of its neutrality and hence, make it susceptible to attack.

Foreign national law is another hurdle the Operational Commander must circumvent to wage network attack. The U.S. has been very successful at getting foreign countries to support rigorous computer intrusion laws.[27] These laws must be taken into consideration when U.S. forces are deployed to a foreign country. One concern is that if network attacks are a violation of foreign national law, the persons issuing the order and those executing it may be criminally liable. Although Status of Forces Agreements (SOFA) between the U.S. and host countries

normally provide complete immunity for host country laws for U.S. personnel performing official duties, we do not have SOFAs with most countries and one may not be obtainable in time to support an operation. In addition, the Operational Commander may feel obligated to conduct operations within the host nation's law, even though he may be legally exempt. Wording is included in most U.S. SOFAs similar to Article II of the NATO SOFA which states:

> "It is the duty of a force and its civilian component and the members there of as well as their dependents to respect the law of the receiving State..." [28]

The result is that since it is unlikely the U.S. will violate a host nation's law, the Commander will be restricted in his ability to implement a network attack. [29]

VI. NETWORK ATTACKS DURING THE KOSOVO CONFLICT

The Kosovo conflict demonstrated that the U.S. has not been completely paralyzed by the legal swirl around offensive network warfare as a combat weapon. General Shelton, Chairman of the Joint Chiefs of Staff, recently informed the media that the U.S. waged Information Warfare as part of the NATO bombing campaign against Yugoslavia in the spring of 1999.[30] However, success of the attack, which was designed to insert false images and targets in the enemy air defense networks, was difficult to ascertain. Although all elements were in place, political hesitations prevented the operation from beginning when the conventional bombing started. By the time the attack was initiated, damage to command lines and other systems by conventional weapons made assessment of the network attack damage "difficult." [31]

While not completely paralyzed, it is obvious that a network attack on one system after it was mostly destroyed by kinetic weapons is not utilizing network warfare to it full potential. General Wesley Clark, NATO Supreme Commander in Europe, criticized the U.S. Kosovo

strategy and commented that more could have been done to "electronically isolate" Milosevic and perhaps even get him to surrender before the bombing campaign started.[32] And recently, Pentagon officials have admitted an all out computer attack on Serbian networks was withheld due to uncertainties and limitations in the emerging field of information warfare.[33] Besides legal issues, other factors have surfaced that could have played a significant role in curtailing network warfare's implementation during the Kosovo operation.

Some military analysts believe the U.S. was as concerned about the prospective loss of its technological lead as it was about legal issues associated with computer attacks.[34] Once the U.S. demonstrates its potential, enemies could easily and cheaply develop defenses and duplicate the capability. The potential for the enemy to retaliate with computer network attacks of its own is another operational reason to carefully weigh the decision to initiate a network attack.[35] Other reasons put forward for the minimal computer attack effort in Kosovo include the untested state of the U.S. arsenal,[36] the lack of a national strategy,[37] and the IW operations approval cycle, which Major General Ronald Keys, the U.S. European Command's director of operations for the Kosovo, identified as a "religious experience."[38] But as will be seen, some of the rationale given for the limited network warfare implemented in Serbia are at least indirectly linked to network warfare's legal issues.

The lengthy IW approval process cited by General Keys was a significant drawback in the computer attack operations in Kosovo. Comments by General Richard Myers provide insight on the cause of the problems when he stated "We worked through some policy and legal issues during Kosovo that will hopefully help us in the future."[39] While the practice of attacks undergoing legal reviews is not new, in fact during the Persian Gulf War, every target underwent a legal review,[40] computer attacks are different. There is a vast mismatch between technological

development (what we can do) and legal development (what is humane and legal).[41] The result is a lengthy review process which delays the network attack targeting approval cycle. This lengthy approval cycle also impedes the establishment of a ready, tested "arsenal" of preplanned attacks that can be utilized during future conflicts.

The void of a national IW strategy is due, at least in part, to a reluctance to "institutionalize" the concept resulting from political and policy concerns.[42] These concerns stem from the unknown political reaction of the international community, which includes the legality element of an attack. For the limited operation in Kosovo, it is difficult to ascertain the lack of a national IW strategy's impact on network attack operations, however, it has been formally addressed by assigning the U.S. Space Command the computer attack mission, which will include forming a national strategy.[43]

However, not all the reasons stated earlier for the limited network attacks are associated with legal issues. The idea that the U.S. is withholding network attacks out of fear the enemy will learn the United States' capabilities and develop a defense or duplicate ability has nothing to do with legal issues, but it, too, can also be discounted. In a global economy, money can buy the best computer talent in the world. States have no need to duplicate the U.S. capability, they can build their own, cheaply and easily. Additional rationale for discounting this explanation is networks are generally unique and has different strengths and vulnerabilities from a security standpoint. An adversary would learn little by studying an attack on a particular system because that weakness may not even exist on their system

Network attack retaliation is another factor that could have influenced implementation of an offensive of network attack. As the most computer and information dependent country in the world, and with numerous military systems relying on civilian infrastructure, the U.S. is also the

most vulnerable to network attack. Military sources have said that if the U.S. cannot defend or adequately counter a network attack, it probably will not initiate one.[44] The flaw with this rationale is it assumes an adversary will retaliate a computer attack with a computer attack. There is no basis for this assumption. If an adversary is going to retaliate, they will use whatever means available to achieve their ends, regardless of how the attack was initiated. Of course, if the original attack was not viewed as legal, the international community would condemn the illegal attack and it could be used as justification for an adversary to retaliate in any manner he is able.

Perhaps the strongest factor outside of the legal issues for the limited network attack was the Yugoslavia infrastructure. An underlying assumption for computer attack as a method of warfare is that the infrastructure and military support systems are computerized and networked, hence, are vulnerable to a computer attack. Some sources have said that this mold did not apply to Yugoslavia.[45] This factor is of particular significance because if this method of warfare did not apply to Yugoslavia, it probably will not apply to the majority of future small, regional conflicts.

Although not identified as a factor in the Kosovo operation, another factor that has the potential to influence network warfare is a relatively new phenomenon: the public's increasing sensitivity to casualties.[46] On the surface, this phenomenon would seem to support network attack as the weapon of choice. As General Richard Myers, Commander in Chief of Space Command said,

> "[information warfare] might be a very elegant way to do it as opposed to dropping a 2,000-pound bomb on Radars for instance...preventing casualties on our side and collateral damage on the adversary's side."[47]

The results of this hypersensitivity have already been seen in Somalia, where the image of a dead U.S. soldier provided the impetus for U.S. withdrawal from that country.[48] But, on the other hand, an unforeseen, cascading effect of a network attack which causes civilian suffering or

death, such as the scrambling of administrative data bases at a hospital which cause the wrong treatments to be administered, could cause a public backlash on the use of computer attack as a weapon. In the extreme case, a catastrophic cascading effect could place a network attack in the category of a weapon of mass destruction. Since the detailed knowledge of an adversary's computer systems is seldom known, the concern of a negative public response may cause reluctance to initiate the aggressive attacks required to achieve measurable results.

VII. CONCLUSION

The requirements of the LOAC place restrictions on the implementation of network attacks. The inability to determine when lower level attacks will be judged "armed attacks" limits their potential use prior to hostilities erupting. The prediction of collateral damage prior to an attack, which is necessary to ensure the requirements of proportionality are met, is especially difficult when civil and military systems are either networked or share computer resources. Additionally, the unforeseen propagation of some types of attacks, such as viruses, could be deemed indiscriminate and limit their applicability to only a limited number of enemy systems. All these factors taken together serve to make the network attack legal review process so lengthy and stringent that, pending significant improvements in our ability to isolate and localize effects, few attacks will ever be deemed legal.

Examples of methods to maximize network warfare's potential in today's setting include the consideration of network attack during the early planning stages, so potential targets can be identified, researched, and an attack plan developed and approved. If time is a factor, targets which have minimal legal implications (pure military systems or those least likely to cascade into civilian systems) should be identified first. These targets will have the greatest probability of

having an attack available in the time required to support an operation. Additionally, establishing a priority based on phasing (when the attack is required) vice the military significance may be useful to enhance the probability the attack will be available when the optimum time to execute it arrives.

The aspects of sovereignty and neutrality must be addressed early in the conflict planning phase and either resolved or limitations established so that effort is not wasted on attack planning that will never be implemented. The resolution of these issues may require significant time, resources and other agency assistance. These issues may ultimately require network attacks be initiated from a different geographic location than the conflict, increasing the Command and Control complexity.

The selection of targets by the Operational Commander can also play an essential role in the future acceptability of network attack by the international community. Damage that can be readily assessed to network attacks and shown to be more humane than a kinetic weapon attack could be extremely valuable. In addition to the short-term political benefits, these types of attacks could provide precedents that would incrementally expand the range of acceptance of future network attacks.

Currently only our own interpretation and application of the LOAC exists for guidance in the legal evaluation of network attacks. While failure to apply the law correctly could have disastrous results in the international arena, failure to realize the potential of this new tool in the battlefield will have equally disastrous results by producing unnecessary casualties and collateral damage. By understanding the rationale behind the limitations imposed on network attacks and the current legal review process, the Operational Commander can maximize network attacks in today's environment

NOTES

1. Bruce D. Berkowitz, "Warfare in the Information Age," Issues in Science and Technology, Fall 1995, 60.

2. Steve Goldstein, "Pentagon Planners Grid for Cyber Assault," Philadelphia Inquirer, 1 December 1999. <http://ebird.dtic.mil/Dec19999/e19991201planners.htm> (1 December 1999), 3.

3. Robert G. Hanseman, "The Realities and Legalities of Information Warfare," The Air Force Law Review, 1997, 3.

4. Dan Kuehl, "The Ethics of Information Warfare and Statecraft," <http://www.infowar.com/MIL_C4I/mil_c4ij.html-ssi> (3 January 2000), 3.

5. Bill Gertz, "U.S. Set to take Warfare On-Line," The Washington Times, 6 January 2000, <http://ebitrd.dtic.mil/Jan2000/e20000106usset.htm> (6 January 2000), 1.

6. United States Naval War College, "Extracts for Instructional Joint Strategic Capabilities Plan FY 1996 'Flexible Deterrent Options,'" reprinted from Instructional Joint Strategic Capabilities Plan FY 1996, NWC 2-96, App. B to Encl. C. Published by the Office of the Joint Chiefs of Staff, Washington, D.C.

7. Lawrence T. Greenberg, "Information Warfare and International Law," National Defense University Press, April 1998, Chap 1, p 4.

8. United Nations Charter, article 2, paragraph 4, states: "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 other manner inconsistent with the Purposes of the United Nations."

9. Phillip A. Johnson in Hanseman, Ibid, 6.

10. Office of General Counsel, Report on an Assessment of International Legal Issues in Information Operations (Washington, D.C., May 1999), 16.

11. John H. Miller, "Information Warfare: Issues and Perspectives," Sun Tzu Art of War in Information Warfare, March 1995, <HTTP://ndu.edu/inss/siws/ch7.html> (27 December 1999), 8.

12. United Nations Charter, Article 39.

13. United Nations Charter, Article 51.

14. Hanseman, Ibid, 5.

15. Howard S. Levis, "Protection of War Victims: Protocol 1 to the 1949 Geneva Conventions." Diplomatic Conference on the Reaffirmation and Development of International Humanitarian

Law Applicable in Armed Conflicts, Geneva, 1974-1977. (Dobbs Ferry, NY: Oceana Publications, Inc., 1979). Articles 48-58.

16. Martin D. Dupuis, John Q. Heywood and Michele Y.F. Sarko. " The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions," American University Journal of International Law and Policy, Vol 2, 1987, 422, 426. The State Department Deputy Legal Advisor made a statement during the conference regarding which principles of Protocol I should be recognized as customary international law. These areas included the civilian population should not be the subject of threats or violence with the purpose to spread terror, attacks should not be carried out that would clearly result in a disproportionate civilian damage, civilians not be used as military shields and that immunity not be extended to civilians taking part n hostilities.

17. Office of General Counsel, Ibid, 6.

18. Ibid, 8.

19. Hanseman, Ibid, Part of the discussion of proportionality and humanity were drawn from Hanseman, 7-8.

20. William Church, "Information Operations Violates Protocol 1," Center for Infrastructure Warfare Studies, <http://www.infowar.com/info_ops/io_and_violations _of_protocol_i1.shtml> (3 January 2000), 4.

21. Levis, Ibid, article 51(3), Vol III, 174.

22. Ibid, article 57 2 (b), Vol III, 337.

23. Office of General Counsel, Ibid, 8.

24. Greenberg, Ibid, The discussion of international laws and treaties and their effect on computer attack is drawn in part from various portions of Greenberg's presentation of Information Warfare and the conduct of Information Warfare and International Law, chap 1 and 2.

25. Hague Convention (V), Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (1907), article 1.

26. Hague Convention (V), Ibid, article 8.

27. Office of General Counsel, Ibid, 34

28. A portion of article II of the NATO Status of Forces Agreement quoted in Greenberg, Ibid, 43.

29. Office of General Counsel, Ibid, 36.

30. William M. Arkin, "The Cyber Bomb in Yugoslavia," Washington Post.Newsweek Interactive, 25 October 1999, <http://www.infowar.com/itftp/c4i/VO2_1125.txt> (29 December 1999). 1.

31. Julian Borger, "Pentagon Kept the Lid on Cyberwar In Kosovo," Guardian, 11 September 1999, < http://www.infowar.com/MIL_C4I/99/mil_c4I_110999a_j.shtml> (3 January 2000), 2.

32. Ibid, 1.

33. Reuters News Service, "U.S. Military Grapples with Cyber Warfare Rules," 8 November 1999, <http://www.infowar.com/MIL_C4I/99/mil_c4i_110899b_j.shtml> (29 December 1999), 1.

34. Borger, Ibid, 1.

35. Berkowitz, Ibid, 60-61. The dependency of CONUS military on civilian infrastructure places the infrastructure systems at risk as potential targets. Examples include commercial communication systems, which carry over 95% of U.S. military communications, transportation systems which, similar to large industrial operations, carry the "just in time" supply materials the military requires, and commercial electrical power sources which supply virtually all military bases.

36. "U.S. Military Grapples with Cyber Warfare Rules," Reuters News Service, 8 November 1999, <http://www.infowar.com/MIL_C4I/99/mil_c4i_110899b_j.shtml> (29 December 1999), 1.

37. Arkin, Ibid, 1.

38. Ronald Keys quoted by Elaine M. Grossman, "Air Force General Found Information Tools A Mixed Bag In Kosovo War," Defense Information and Electronics Report, 7 January 2000, 1.

39. Richard Myers, "Current Activities of the U.S. Space Command," Department of Defense News Briefing, <http://www.defenselink.mil/news/Jan2000/t01052000_t104myer.html> (7 January 2000), 9.

40. Chuck Homer quoted in Hanseman, Ibid, 14.

41. Hanseman, Ibid, 5.

42. Bob Brewin and Heather Harreld, "DOD Adds Attack Capability to Infowar," 2 March 1998, <http://athena.fcw.com> (27 December 1999), 1.

43. Myers, Ibid, 3.

44. Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force," Naval War College Review, Spring 1998, 5.

45. Gertz, Ibid, 2.

46. Charles J. Dunlap, "Sometimes the Dragon Wins: A Perspective on Information Warfare,"

1996, <http://www.infowar.com/MIL_C4I/DRAGON.html-ssi> (29 December 1999), 10.

47. Ibid, 1.

48. Jeffrey Record, "Congress, Information Technology, and the Use of Force, " Information Age Anthology ed. David S. Alberts and Daniel S. Papp, June 1997, <http://www.dodccrp.org/antch17.html> (29 December 1999), 6.

BIBLIOGRAPHY

Arkin, William M. "The Cyber Bomb in Yugoslavia." Washington Post.Newsweek Interactive. 25 October 1999. <http://www.infowar.com/itftp/c4i/VO2_1125.txt> (29 December 1999).

Arquilla, John J and David F. Ronfeldt. "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict." RAND Research Review. Fall 1995. <http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html> (27 December 1999).

Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force." Naval War College Review, Spring 1998.

Berkowitz, Bruce D. "Warfare in the Information Age." Issues in Science and Technology, Fall 1995, 59-66.

Borger, Julian. "Pentagon Kept the Lid on Cyberwar In Kosovo." Guardian. 11 September 1999. <http://www.infowar.com/MIL_C4I/99/mil_c4I_110999a_j.shtml> (3 January 2000).

Brewin, Bob and Heather Harreld. "DOD Adds Attack Capability to Infowar." 2 March 1998. <http://athena.fcw.com> (27 December 1999).

Campen, Alan D. "Rush to Information Based Warfare Gambles with National Security." Signal, Jul 1995, 67-69.

Carey, Anne R. "Computer Virus." USA Today, 8 December 1999, section B, p 1:1.

Chairman of the Joint Chiefs of Staff. Implementation of the Law of War. CJCSI 5810.01A. Washington: 1999.

Church, William, "Kosovo and the Future of Information Operations." Center for Infrastructure Warfare Studies. <http://www.inforwar.com/info_ops/treatystudyio.shtml> (3 January 2000).

_____ "Information Operations Violates Protocol 1." Center for Infrastructure Warfare Studies. 23 June 1999. <http://www.infowar.com/info_ops/io_and_violations _of_protocol_i1.shtml> (3 January 2000).

Crawford, J.W., "The Law of Noncombatant Immunity and the targeting of National Electric Power Systems." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

Dunlap, Charles J. "Sometimes the Dragon Wins: A Perspective on Information Warfare." 1996, <http://www.infowar.com/MIL_C4I/DRAGON.html-ssi> (29 December 1999).

Dupuis, Martin D., John Q. Heywood and Michele Y.F. Sarko. " The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions." American University Journal of International Law and Policy, Vol 2, 1987, 415-426.

Gertz, Bill. "U.S. Set to take Warfare On-Line." Washington Times. 6 January 2000. <http://ebitrd.dtic.mil/Jan2000/e20000106usset.htm> (6 January 2000).

Goldstein, Steve. "Pentagon Planners Grid for Cyber Assault." Philadelphia Inquirer. 1 December 1999. <http://ebird.dtic.mil/Dec19999/e19991201planners.htm> (1 December 1999).

Gompert, David C. "Keeping Information Warfare in Perspective." RAND Research Review. Fall 1995. <http://www.rand.org/publications/RRR/RRR.fall95.cyber/ perspective.html> (3 January 2000).

Greenberg, Lawrence T. "Information Warfare and International Law." National Defense University Press, April 1998.

Grossman, Elaine M. "Air Force General Found Information Tools A Mixed Bag In Kosovo War." Defense Information and Electronics Report. 7 January 2000.

Hague Convention (V). Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (1907), Articles 1-25.

Hanseman, Robert G. "The Realities and Legalities of Information Warfare." The Air Force Law Review, 1997, 173-200.

Hultman, Evan L. "The Law of Armed Conflict in Modern Armed Forces." The Officer, November 1997, 29-35.

Joint Chiefs of Staff Publication 6-0. Doctrine for Command, Control, Communications, and

Computer (C4) Systems Support to Joint Operations, Washington D. C.: May 1995.

Koch, Andrew. "USA to Form New Warfare Center." Jane's Defense Weekly, 13 October 1999.

Kuehl, Dan. "The Ethics of Information Warfare and Statecraft." <http://www.infowar.com/MIL_C4I/mil_c4ij.html-ssi> (3 January 2000).

Libicki, Martin C. "The Next Enemy." Strategic Forum number 35. July 1995. <http://www.dodccrp.org/libicki1.htm> (3 January 2000).

Levis, Howard S. "Protection of War Victims: Protocol 1 to the 1949 Geneva Conventions." Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva, 1974-1977. Dobbs Ferry, NY: Oceana Publications, Inc., 1979.

Miller, John H. "Information Warfare: Issues and Perspectives." Sun Tzu Art of War in Information Warfare. March 1995. <HTTP://ndu.edu/inss/siws/ch7.html> (27 December 1999).

Myers, Richard. "Current Activities of the U.S. Space Command." Department of Defense News Briefing. <http://www.defenselink.mil/news/Jan2000/ t01052000_t104myer.html> (7 January 2000).

Nelson, Bradford K. Applying the Principle of War in Information Operations. <http://www-cgsc.army.mil/milrev/English/SepNov98/nelson.htm> (27 December 1999).

Office of General Counsel. Report on an Assessment of International Legal Issues in Information Operations. Washington, D.C., May 1999.

Owens, William A., "The Emerging U.S. System-of-Systems." National Defense University Strategic Forum. <http://www.ndu.edu/inss/strforum/forum63.html> (14 January 2000).

RAND Research Review. "That Wild, Wild Cyberspace Frontier." Fall 1995. <http://www.rand.org/publications/RRR/RRR.fall95.cyber/wild.html> (27 December 1999).

Record, Jeffrey. "Congress, Information Technology, and the Use of Force." Information Age Anthology ed. David S. Alberts and Daniel S. Papp. June 1997. <http://www.dodccrp.org/antch17.html> (29 December 1999).

Reisman, Michael W. and Chris T. Antoniou, ed. Legal Rules on Armed Conflict—The Laws of War. Cambridge, MA: Nieman Reports, 1994.

The Joint Staff. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd ed. Washington D.C.: 1996.

Reuters News Service. "U.S. Military Grapples with Cyber Warfare Rules." 8 November 1999. <http://www.infowar.com/MIL_C4I/99/mil_c4i_110899b_j.shtml> (29 December 1999).

U.S. Navy Department. The Commander's Handbook on the Law of Naval Operations (NWP 1-14M). Washington, D.C.: October 1995.

United Nations Charter. June 1945. <http://www.unm.edu/humanrts/instree/aunchart.htm> (11 January 2000).

United States Naval War College. "Extracts for Instructional Joint Strategic Capabilities Plan FY 1996 'Flexible Deterrent Options.'" reprinted from Instructional Joint Strategic

Capabilities Plan FY 1996. NWC 2-96, App. B to Encl. C. Published by the Office of the Joint Chiefs of Staff, Washington, D.C.

Wilson, Michael. "Waging IWAR." 7Pillars Partners. <http://www.7pillars.com/papers/Waging.html> (27 December 1999).

Zengel, Patricia, "Responding with Force to Information Warfare: Legal Perspectives." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1997.