STRATEGY RESEARCH PROJECT

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

THE INTERNATIONAL LEGAL IMPLICATIONS AND LIMITATIONS OF INFORMATION WARFARE: WHAT ARE OUR OPTIONS?

BY

LIEUTENANT COLONEL BRYAN W. ELLIS
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2001

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

20010430 118

USAWC STRATEGY RESEARCH PROJECT

The International Legal Implications and Limitations of Information Warfare: What Are Our Options?

by

LTC Bryan W. Ellis
U.S. Army

COL Ralph Ghent
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

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

ABSTRACT

AUTHOR: LTC Bryan W. Ellis

TITLE: The International Legal Implications and Limitations of Information Warfare: What Are Our Options?

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 28 CLASSIFICATION: Unclassified

When we examine the relationship between information warfare (IW) and the law, particularly international law and the law of war, it becomes apparent that fundamental questions need to be explored. How is "war" defined as it relates to IW and what activities will we define as IW? Who are considered combatants in IW? How do the terms "force," "armed attack," or "aggression" equate or relate to IW? Does "war" require physical violence and human casualties? How will established legal principles related to national sovereignty be affected by IW? These questions and issues merely hint at the tremendous uncertainties surrounding the evolving discipline of IW.

This paper examines IW from a layman's legal perspective and explores issues such as the law of war and standing international agreements to which the United States is a signatory. The concept for the employment of IW is evolving and as recently demonstrated in Yugoslavia, legal constraints, limitations, and issues appear to be the norm. There is currently no authoritative legal or international agreement as to whether an IW "attack" is comparable to an "attack" or "use of force" in the traditional sense.

With this as a context, the study identifies several legal approaches our armed forces could employ offensively, defensively, or in retaliation to an information attack.

TABLE OF CONTENTS

ABSTRACT iii

THE INTERNATIONAL LEGAL IMPLICATIONS AND LIMITATIONS OF INFORMATION WARFARE: WHAT ARE OUR OPTIONS? 1

INTERNATIONAL LAW 2

THE LAW OF NATIONS 2

THE LEGAL CHALLENGES OF INFORMATION WARFARE 2

THE LEGALITY OF INFORMATION WARFARE AND INTERNATIONAL TELECOMMUNICATIONS LAW 3

MAJOR LIMITATIONS ON INFORMATION WARFARE 4

Neutrality and National Sovereignty 4

International Humanitarian Law 5

Foreign Domestic Laws 6

INTERNATIONAL LEGAL REGULATION OF THE USE OF FORCE IN PEACETIME-PROBLEMS OF DEFINITION 6

Is Information Warfare "Warfare"? 7

The Importance of Categorization 8

Response to Information Warfare Attacks 9

Identification of an Attack 9

Investigation of Network Attacks and the Problem of Territorial Jurisdiction 9

Cooperation 10

Retaliation and Reprisals 11

What Are Our Options? 12

Resolve Legal Ambiguities 12

International Cooperation 13

Protection of Critical Systems 14

Ban Or Limit the Weapons of Information Warfare 14

Complacency 14

CONCLUSION 15

ENDNOTES 17

BIBLIOGRAPHY 21

THE INTERNATIONAL LEGAL IMPLICATIONS AND LIMITATIONS OF INFORMATION WARFARE: WHAT ARE OUR OPTIONS?

> "If we can drop a bomb on it, why can't we take it out by a computer network attack?"[1]
>
> — unknown U.S. military planner

In the spring of 1999, the Pentagon considered hacking into Serbian computer networks to disrupt their military operations and basic civilian services in support of Operation Allied Force. Prior to execution, however, the effort was halted because of continuing uncertainty and limitations surrounding the emerging field of information warfare (IW).[2]

As computers continue to revolutionize and impact virtually every aspect of our lives, military planners have stepped up development of information weapons and speak of their potential to change the nature of war. Instead of risking planes and pilots to interdict power grids, rail lines, and telephone exchanges, planners envision IW soldiers stealthily invading computer networks to shut down electrical facilities, interrupt phone service, and disrupt national financial systems.[3]

In May 1999 (updated November 1999), the Department of Defense Office of General Counsel issued guidelines warning that misuse of information attacks could subject U.S. authorities to war crimes charges. It advised commanders to apply the same "law of war" principles to computer attacks that they do to the use of bombs and missiles. These call for hitting only targets of military significance, minimizing collateral damage, and avoiding indiscriminate attacks.[4]

Yet the question posed by the military planner in the opening epigraph has become a recurring theme. In some instances a computer network attack may be a viable option, but we must still conduct such an attack in accordance with the law of armed conflict and ensure collateral damage is limited. Sounds easy enough, but compliance with the law, especially minimizing collateral damage, is extremely difficult in light of the fact that many military communications systems transit civilian computer networks. Collateral damage then becomes almost unavoidable.

Currently, our ability to utilize information warfare as an offensive capability is hamstrung by a myriad of legal issues. Conversely, our ability to militarily respond to an information attack is equally as hamstrung by the legal system.

This study investigates the legal implications and limitations of both offensive and defensive IW. It also offers several legal approaches the U.S. could employ to protect the military information infrastructure and clarifies options useful for offense, defense, or retaliation.

The study is intentionally limited in two areas: First, the definition of IW is based on those in Martin Libicki's What is Information Warfare?, where he describes seven distinct forms of IW.[5] To limit its scope, this study includes no discussion or reference to electronic, psychological, and economic IW.[6] Second, the study includes no discussion of international law regulating activities in space. No doubt, there is a strong imperative to interfere with space-based information systems belonging to an adversary, and an equal imperative to defend our own.

INTERNATIONAL LAW

THE LAW OF NATIONS

Law governs war as it does most human endeavors. International law governs the interaction among nations and consists primarily of "conventional" and "customary" law.[7] Conventional law is enacted by treaty or other explicit agreement among nations. Customary law, on the other hand, is derived from an interpretation of treaties or agreements, declarations of international bodies such as the General Assembly of the United Nations, or the statements and actions of governments and their officials. Customary laws can also be defined as mere manifestations of accepted traditional international practice.[8]

It is important to understand that international law, in terms of national security, is not a body of law created by legislatures and enforced through a court system. Rather, international law is generally established by agreement among the parties who will be bound by it, much like private parties entering into a contract. Although legal forums such as the International Court of Justice do exist, their enforcement mechanisms are limited. Consequently, a country willing to accept the political and diplomatic consequences of their actions may act accordingly, relatively unrestrained. It is likely that nations will violate the dictates of international law when those dictates endanger or conflict with the pursuit of their fundamental interests, including national security.[9]

THE LEGAL CHALLENGES OF INFORMATION WARFARE

The advent of information technology makes it possible for adversaries to attack each other in new ways, inflicting new forms of damage. Attackers may use international networks to damage or disrupt enemy systems without ever physically entering the enemy's country. Additionally, a country's dependence on information-based systems may make those systems

particularly attractive targets. Furthermore, the dual-use nature of many information systems and infrastructures may blur the distinction between military and civilian targets.[10]

So prospects of new technological attacks may pose problems for international law because law is inherently conservative. Technological change may enable new activities that do not fit within existing legal categories, or may reveal contradictions among existing legal principles.

IW challenges existing international law in three primary ways: First, the intangible damage that information attacks may cause is fundamentally different than the physical damage caused by traditional warfare. The damage and destruction caused by conventional munitions is easy to comprehend and conforms with accepted views of war. In contrast, the disruption of information systems or the manipulation or corruption of stored or transmitted data may cause intangible damage, such as the disruption of civil or government services.[11]

Second, the ability of information or an electronic signal to transit international networks challenges the concept of national or territorial sovereignty. As the world becomes increasingly "networked" with signals traveling across international borders with impunity, allowing individuals or groups to affect systems around the globe, the precept of sovereignty becomes blurred, since national legal authority generally applies only within national borders. Additionally, the intangible violation of national borders that information flow may cause may not be the type of violation traditionally understood to be part of a military attack.[12]

Third, just as information attacks may be difficult to define as "war," it is equally as difficult to define targets as military, thus legitimate, or civilian, which are generally forbidden. Furthermore, the intangible damage caused by information attacks may not result in the sort of injuries to noncombatants that humanitarian law is designed to protect.[13]

THE LEGALITY OF INFORMATION WARFARE AND INTERNATIONAL TELECOMMUNICATIONS LAW

As a result of the rapid technology expansion of the past decade, no provision of international law explicitly prohibits what we know as IW. The absence of prohibitions is significant because that which international law does not specifically prohibit, it tacitly permits.[14]

A network attack may involve the International Telecommunications Union (ITU) and its underlying charter, the International Telecommunications Convention (ITC), which applies to international wire and radio frequency communications. In practice, the ITU may not substantially limit IW activities.[15] The primary concerns of the ITU are interoperability and interference.[16] Regulations promulgated under the ITU have some applicability to information

attacks that use the electromagnetic spectrum or international telecommunications networks. Broadcasting stations from one nation may not interfere with broadcasts of other states' services on their authorized frequencies.[17] Additionally, governments must protect the secrecy of international correspondence, although they retain the right to stop radio or wire transmissions for national or domestic security purposes.[18]

The preceding provisions would seem to prevent the disruption of an adversaries' telecommunications. But in practice, they may not.[19] First, the rules against interference do not apply to belligerents, so wartime communications are fair game. Secondly, even in peacetime, violation of the ITU rules and regulations may have limited repercussions, especially for a country with as significant a role in the international telecommunications arena, such as the U.S..[20] Even if international sanctions or condemnation appeared likely, the U.S. might decide that the repercussions it will face from external interference would not outweigh its need to conduct operations against a particular adversary. Finally, it is important to note that even if IW activities violate the ITU rules and regulations, they may be considered merely a breach of contractual obligation under treaty rather than an act of war, which would justify a forceful response,[21] although a contractual dispute would not justify such a response.

MAJOR LIMITATIONS ON INFORMATION WARFARE

Despite the novelty of some IW techniques, international law currently places some constraints on the conduct of IW, just as it does on traditional forms of warfare. However, characteristics of IW pose problems for those who attempt to use international law to limit IW and provide considerable legal latitude for those who choose to wage such warfare.[22]

Neutrality and National Sovereignty

The territory of neutral states is supposed to be inviolate to the force of belligerents by both treaty and longstanding customary law.[23] If IW is viewed as an instrument of force, it is arguable that a belligerent is therefore prohibited from channeling an attack through the networks of a neutral state. Conversely, a neutral's failure to resist the use of its networks for attacks against another country may make it a legitimate target for reprisals by the country that is the ultimate target of the attacks.[24]

The argument that an electronic incursion is a violation of neutrality is supportable, but the counterargument is that historically violations of neutrality meant a physical violation of a nation's borders, not an electronic intrusion. Information attacks occur in another dimension, and the general consensus is that current law is not applicable.[25] Attacking a neutral nation's

computer network might not violate its neutrality because it involves no physical encroachment. A neutral nation has no obligation to resist a belligerent's use of its "publicly accessible communications equipment."[26] Since computers are used to communicate, the logical conclusion might be that they fall under this exception and therefore can be used by a belligerent. On the other hand, computers may be distinguishable since they can be used as weapons, whereas other communications devices may not.[27] Again, it is unclear where IW falls.

With the increasing cost and huge investment required for advanced technology, many countries have joined to establish international consortia, further complicating the issue of neutrality. When an international communications system is developed by a military alliance such as NATO, few neutrality issues are likely to arise. Other international consortia, however, provide communications and data that are used by both civilian and military organizations. The mere breadth of membership in these consortia virtually guarantees that not all members will be allied in future conflicts.[28]

International Humanitarian Law

The fundamental principle of international humanitarian law would appear to welcome the non-lethal destruction that IW promises as an alternative to the violence and devastation of traditional wars. But that body of law, a combination of conventions and longstanding customary law,[29] may constrain IW just as it does traditional warfare. The fundamental principle of humanitarian law is that there are limits to the methods that can be used against adversaries during war and that the cruelty of war must be mitigated and circumscribed.[30]

Although humanitarian law protects both combatants and noncombatants, the most significant relevant general tenet of humanitarian law is the protection of civilians. This concept was originally codified in the St. Petersburg Declaration of 1868, which "recognized that the only legitimate object of war was to weaken an enemy's military forces."[31] Civilians, as such, may not be the object of an attack.[32] Because of the concern over attacking proper objectives, humanitarian law requires that nations use weapons that allow aggressors to distinguish between military and civilian targets. The problem is that both the military and civilians use many of the same information systems. Thus it is unclear whether these "dual-use" systems can be attacked.[33]

For example, according to customary international law, it is legal for warring parties to cut off lines of communication. Thus, actions taken to destroy or inhibit the lines of communication between military systems would most likely be permissible because they are a major military objective. But weighed against the potential harm to civilians subjected to an information attack,

this proposition becomes debatable. For example, a virus unleashed on a dual-use system might inhibit both its military and civilian functions, potentially causing great civilian hardship.[34]

Humanitarian law also requires that the aggressor abide by the principle of "proportionality" between civilian damage and the military objective attained. The principle requires that parties responding to attacks consider whether the force in response is proportional to the wrong, or whether a given action is appropriate in light of its objectives and the resultant casualties.

The applicability of this principle to IW is important for two reasons: First, it creates difficult issues for those that seek to attack dual-use targets. If the principle does not apply to IW, attackers do not have to be concerned with civilian losses. Second, if IW is covered, it will be difficult to weigh whether the type of response is appropriate.[35]

We have noted that one of the basic tenets of international law is that attacks against civilians are prohibited. However, civilians and civilian property that make a direct contribution to the war effort may be targeted. The corollary of this principle is that civilian systems that have no direct contribution to the war effort, and whose destruction would provide no significant military advantage to the attacker, are immune from deliberate attack. This creates a dilemma for the military commander contemplating an information attack against a country's financial, transportation, or communications systems. To observe the law, the commander must show clear military necessity in the damage or destruction of these services.

Foreign Domestic Laws

Laws enacted by other nations may limit information warfare conducted by U.S. military forces. Current U.S. criminal statutes apply to information operations. Similarly, foreign criminal statutes will most likely apply to U.S. information operations activities.[36] There is enormous variation, from country to country, regarding foreign domestic law governing high-tech activities. This has important implications for U.S. information operations for two basic reasons: First, a nation's domestic criminal law directly affects the assistance that the nation can provide in suppressing certain behavior by persons operating in its territory. Second, a nation's domestic law may limit U.S. information operations conducted in the nation's territory or involving communications routed through the nation's communications systems.[37]

INTERNATIONAL LEGAL REGULATION OF THE USE OF FORCE IN PEACETIME-PROBLEMS OF DEFINITION

As discussed in the previous section, a nation engaged in an international armed conflict can attack lawful military targets. Resolutions of the United Nations Security Council (UNSC)

may also authorize the use of armed force as provided in the U.N. Charter. But how does international law apply in situations where there is no armed conflict or UNSC mandate, ranging from peacetime to military operations other than war?[38]

Is Information Warfare "Warfare"?

One effect of technological change is that the new activities that it enables may not fit within established legal categories. A fundamental question that arises from the development of IW techniques is one of definition. Has the development of IW technology and techniques removed IW from the existing legal definition of war? It's not obvious that all information attacks, including some that could inflict serious damage, reside with what has previously been our understanding of "war."[39] Similarly, the extent of the damage that such an attack could inflict, particularly upon civilians, may not be the type of hardship that historical and conventional laws of war were intended to alleviate. Consequently, there may be confusion over what limits may apply to the conduct of IW, or under what conditions such attacks may be carried out.[40]

The frequently asked question, "Is a computer network attack an act of war?" is not addressed in the U.N. Charter. Nor is the definition of an act of war addressed in the modern international legal system.[41]

Members of the U.N. have agreed in Article 2, Section 4, of the Charter to "refrain ... from the threat or use of force against the territorial integrity or political independence of any state."[42] Article 51 of the Charter stipulates one exception to the prohibition: "force may be used in self defense of an armed attack."[43] The question is whether IW qualifies as either use of force or an armed attack. Neither the Charter nor the International Court of Justice have defined these terms, making it unclear what constitutes an "armed attack."[44] The term has been construed to require the "use of armed forces, force, or violence, as well as interference with a nation's sovereignty." However, "even actions involving destructive, physical force may not rise to the level of 'armed attack'." Thus, without U.N. clarification, it is unclear whether a nation is legally justified in responding forcefully to an information attack.[45]

The U.N. General Assembly's definition of "aggression" is also unclear. It provides that the U.N. Security Council can address acts of aggression, which are characterized as "the use of armed force by a State against the sovereignty, territorial integrity, ... of another State."[46] It is difficult to say whether IW constitutes aggression, because it is different from the traditional notion of physical warfare. Although IW's results are tangible in a physical sense, the information attack is non-physical, since it is perpetrated through wires and digits. The issue is whether the act or the result is what the words "use of force" are intended to characterize.[47]

Even more confusing is the U.N. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States ("Non-Intervention Treaty").[48] The Treaty prohibits direct or indirect intervention in the "internal or external affairs of any state" and provides that "armed intervention and all other forms of interference ... against a State ... are condemned."[49] The problem with the Treaty is that it does not define intervention nor give a clear indication whether "other forms of interference" constitutes aggression, thereby warranting a response in self-defense under Article 51 of the U.N. Charter.[50] Thus States are left to respond to an attack, not knowing whether it will be considered a violation of international law.

The Importance of Categorization

The issue of how to categorize information attacks is critical. Whether or not an information attack is considered an act of "war," "force," or "aggression" is relevant to whether the use of force can be justified as self-defense and whether a particular response is proportionate to the original attack.[51]

Characterization of attacks is relevant under international humanitarian law, specifically those provisions that protect noncombatants from attacks and the resultant consequences. First, if an information attack is not considered an act of "war," then humanitarian law may not apply. Second, as discussed previously, it is unclear whether the non-physical damage that some information attacks cause are the sort of effects against which humanitarian law protects noncombatants. If humanitarian law does not apply, then countries may legally pursue IW without legal concern for the harm that civilians might suffer.[52]

The difficulty in characterizing certain forms of IW as "force," "war," or "aggression" under international law does not mean that international legal institutions cannot respond to such attacks. Chapter VII of the U.N. Charter gives the U.N. Security Council the authority and responsibility to determine the existence of any "threat to the peace" or acts of aggression,[53] and the Council can recommend and lead an appropriate response.[54] An information attack that may not constitute "force" or "aggression" may be considered a threat to the peace and thus subject to Security Council action, including the use of military force. Any action that might anger a government to the point it might contemplate the use of military action would "threaten" the peace, even if the provocation were not technically illegal. Because Security Council actions are subject to international political negotiation, any response would not likely be quick or a significant deterrent to an aggressor.[55]

RESPONSE TO INFORMATION WARFARE ATTACKS

Most agree that the U.S. leads the world in IW capability, yet other countries, transnational criminal organizations, and terrorist groups are pursuing similar capabilities. Because of the overwhelming traditional military power of the U.S., and because information attacks offer a way for an adversary who can't match the traditional might of the U.S. to strike at the U.S., it is likely that the U.S. will suffer a future serious information attack. If, or more likely when, such an attack occurs, the U.S. may find its response hindered because the international legal system may not have established rules applicable to such an attack.[56]

IDENTIFICATION OF AN ATTACK

The first dilemma in responding to an attack is identifying a specific event as an actual attack. This is exacerbated when an attack occurs during a period of relative calm or reduced international tensions. Investigators may have difficulty distinguishing an accidental catastrophe from one stemming from malice.

Computer-based attacks may be difficult to distinguish from innocent malfunctions. If an attack is carried out across a network, the culprit may never be in physical proximity to the target and may leave no tangible evidence. An attack that uses viruses, logic bombs, or infected software may be difficult to detect quickly, if at all, because of the complexity of systems and the frequency of unintentional errors.[57]

Perhaps the greatest challenge the U.S. faces in presenting evidence of an attack to the international community is that it must not only be sufficient to convince U.S. policymakers, but also to convince foreign governments. There is currently no accepted standard of proof for an information attack in the U.S. or the international community. The deliberations of the U.N. Security Council, as well as those of foreign governments, are political rather than legal. Diplomacy may be more significant than persuasive, logical arguments. And the skepticism of foreign governments towards U.S. intentions and technical methods of detection further complicates the task of investigators and policymakers alike.[58]

INVESTIGATION OF NETWORK ATTACKS AND THE PROBLEM OF TERRITORIAL JURISDICTION

Investigators tracing attacks across computer networks are hamstrung by the fact that networks cross international borders, but the authority of national agents does not. An attack may originate in a foreign country, or may be routed through several countries, but law enforcement or national security personnel can't unilaterally pursue into networks in other countries. We have previously noted that the principle of sovereignty grants each government

exclusive authority over events within its borders.[59] Investigators are thus dependent upon foreign cooperation or, with proper home-country authorization, must operate covertly.

The principle of sovereignty was conceived when international law was concerned with physical intrusion across a nation's borders. Today, most national governments would probably contend that intrusion into their computers or information networks is similar to traditional border violations. Some governments have already enacted data protection codes that forbid the transmission of certain personal data to countries that don't provide sufficient protection for the data.[60] Such governments may consider investigations by foreigners a criminal misuse of their systems and a form of computer crime.[61]

The conflict between international networks and national sovereignty is more than academic. The U.S. government has already pursued foreigners who have entered U.S. computer systems for malicious purposes. The attackers have complicated the investigations by "looping and weaving" through several foreign countries in an attempt to stymie the investigators.[62]

The widespread availability of the technology necessary for international computer attacks, combined with the anonymity provided by technology, complicates the efforts of investigators and makes it difficult to determine responsibility for an attack. The availability of the technology also reduces the need for terrorists to seek state support, while giving states that support terrorism "plausible deniability" in such attacks. Absent a credible admission of responsibility, it may be impossible to attribute an attack to its actual source with any degree of confidence.[63]

COOPERATION

In the absence of an international investigation treaty, countries have no obligation to cooperate with each other in law enforcement or national security investigations. Non-cooperation cannot be considered evidence of implication in an attack. Further, hostile nations may be unwilling to assist foreign investigators, whom they may consider spies.

International law enforcement agreements may not adequately support an investigation. For example, treaties of mutual legal assistance generally contain exceptions that permit parties to refuse cooperation under certain circumstances. In cases where a country may feel they will not be able to adequately monitor or control the investigators' activities, they will certainly take advantage of any loopholes that exist.[64]

Given the challenges to international cooperation discussed above, the U.S. may unilaterally pursue an investigation without the cooperation of foreign countries. Although such

an investigation seems likely to violate the sovereignty of those nations, it would not in itself violate international law. However, some countries could characterize the investigation as espionage, which does not violate international law,[65] but certainly violates, indeed threatens, national sovereignty.

RETALIATION AND REPRISALS

When a state can tie an attack directly to a foreign government, the offended state may retaliate to terminate the ongoing attack. The retaliation may be justified as part of its right to self-defense under Article 51 of the U.N. Charter.[66] However, it is unclear whether Article 51 provides a basis for military response against a state conducting certain information attacks.

Our discussion of "war," "aggression," and "force" has shown how difficult it can be to predict whether specific actions will be considered an "armed attack." International law does not identify mandatory elements of "crimes," while any such determination in forums such as the U.N. will be inherently political and diplomatic. Nevertheless, in all likelihood, an "armed attack" would include some level of physical destruction, combined with some level of intrusion into a state's borders or violation of its sovereign territory.[67]

Attacks such as computer intrusions or communications disruptions are difficult to characterize. A computer intrusion intended to steal data and another intended to disrupt an air traffic control system may be equally intrusive, but the greater level of destruction and death resulting from the disruption of the air traffic control system may make it more likely to be considered an "armed attack" than the data theft. Any sufficiently destructive computer attack may qualify as an "armed attack," no matter what the level of intrusion. But again, we're faced with quantifying "sufficiently destructive."

If a computer attack cannot be characterized as an "armed attack," then a conventional response may not be warranted. A conventional response, in this case, may in fact be considered the "armed attack" under Article 51. A response in kind would not constitute an "armed attack." But if the attacker can be identified, he may lack the information infrastructure that would make him vulnerable to a response in kind.[68]

In addition to the U.N. requirement that force be limited in response to an armed attack, customary international law establishes requirements for retaliation. The retaliation must be in self-defense against the attack, it must be necessary to stop the initial attack or prevent further violations, and it must be proportional to the attack.[69]

Just as it is difficult to determine whether an information attack is an "armed attack," it is equally as difficult to determine what would be a proportionate response to the attack, especially

when the attack inflicts little or no physical destruction. When a computer attack disrupts or corrupts a database or results in denial of important services, a decision must be made regarding what sort of response is appropriate to the original computer attack. In the absence of physical destruction, it is questionable whether the international community would consider a conventional military attack a proportionate response.

The U.S. seems to hold the position that "reprisals involving the use of force are illegal," although it "recognizes that patterns of attack or infiltration can rise to the level of an 'armed attack,' thus justifying a responding use of force in the exercise of the right of self-defense."[70] In other words, the U.S. may be disinclined to characterize an armed attack as a reprisal, labeling it instead as an act of self-defense.

WHAT ARE OUR OPTIONS?

As discussed, international law has yet to resolve ambiguities over the characterization of IW. This ambiguity affords the U.S. and others the opportunity to engage in IW activities, possibly even in peacetime, without significant legal repercussions. Conversely, international law may permit attacks against the U.S., and limit our ability to respond appropriately or effectively, particularly in peacetime.

U.S. policymakers may appreciate the legal status quo. The U.S. appears to lead the world in IW capability, so an international legal regime that permits information attacks offers a distinct advantage. It affords us a technological edge in an international conflict that exceeds the capability of most adversaries.[71]

Given our world position, the U.S. has the opportunity to begin establishing international norms and, perhaps, customary international law. We are currently in the international position of legislator, enforcer, and perhaps executioner to our adversaries. We should, however, not be sanguine about the current state of international law. While our capabilities far outweigh those of our adversaries, our civilian and military systems are largely dependent upon our information infrastructure. If only to increase protection for U.S. systems, certain nonexclusive legal, diplomatic, or policy initiatives seem desirable.[72]

RESOLVE LEGAL AMBIGUITIES

To understand the status of information attacks under international law, it is imperative that the concepts of "armed attack," "aggression," and "force" be clarified. It may be in the best interest of the U.S. to support restrictive definitions of the terms to preserve our technological advantage and protect future technological developments. On the other hand, it may be more

advantageous to support a broad definition to minimize or reduce the legal methods by which an adversary can exploit our information infrastructure.

Any U.S. action to reduce or minimize civilian casualties and suffering will be viewed as a positive step by the international community and may open the way to productive negotiations. Definitions that include non-lethal information attacks within "war" or "force" might offer civilians an element of protection from such peacetime attacks because of the increased political and diplomatic repercussions of such attacks. To increase protection of civilian targets in wartime, the U.S. could pursue treaties or other international agreements that define non-lethal or intangible damage to civilian institutions or infrastructure as the type of injuries against which humanitarian law should protect noncombatants.

The U.S. possesses the legal leverage necessary in the international community to achieve whatever objectives it chooses. The U.S. can also influence the development of customary law regarding IW. The introduction of U.S. views and position in bodies such as the U.N. can potentially influence the opinions of other states, leading to the emergence of international norms regarding IW.[73]

The U.S. must be equally cautious in drawing international attention to the potential dangers of IW. It is possible that potential adversaries may view the U.S. initiative as an effort to protect our technological advantage, which could in turn actually increase their efforts to obtain and use IW weapons.

INTERNATIONAL COOPERATION

If we look to history for solutions, we realize that international cooperation has met with little success in eliminating international acts of terrorism, but has met with some success in stemming certain international acts of terrorism, such as hijacking. A strategy similar to that applied to hijacking can be applied to IW. First, diplomatic pressure must be applied to those nations that do not currently recognize information attacks as a crime.[74] This diplomatic pressure would discourage a passive view towards those involved in IW within their borders and would encourage extradition of the offenders. In addition to diplomatic pressure, a nation's refusal to cooperate with a reasonable investigation could be met with sanctions against the nation. In cases where evidence indicates the nation is shielding individuals who acted on its behalf, the evidence, combined with the refusal to cooperate, should be considered an act of war. Second, the U.S. could support the development of an extradition regime for criminal or terrorist information attacks, requiring the extradition or prosecution of those charged with specific network-related crimes.

PROTECTION OF CRITICAL SYSTEMS

Technology has driven us to a precarious position. More and more critical functions are controlled by networked computer systems, the failure of which can have catastrophic consequences. This is true not only in the U.S., but throughout the developed world. It is reasonable to believe that some of these systems are so critical that countries can agree that they be off limits to information attacks, or that all countries would agree they must cooperate in defending one another's systems.

Systems that might qualify under a protection regime include those involved in command and control of strategic weapons, international finance, financial markets or stock exchanges, telephone switches, emergency communications, rail transport, air traffic control, and medical databases.[75] Such agreements could be pursued under direct U.N. auspices or by means of individual treaties in the context of existing organizations and institutions.

BAN OR LIMIT THE WEAPONS OF INFORMATION WARFARE

An outright ban on IW or placing strict controls on the weapons of IW appears sensible from the U.S. perspective, particularly if we find our vulnerabilities outweigh our technological advantages. A ban also appears logical from an international legal perspective in that it would provide clear norms to guide future actions.

While such an approach seems sensible and logical, it is probably unrealistic. Many IW "weapons" have dual military and civilian uses, with the majority of their applications used by the civilian sector. Many of these "weapons" provide a great capability in the civilian sector and only evolved to be used for other than their intended purpose.

The U.S. must also avoid prematurely limiting a weapon that could potentially offer some measure of non-lethality to conflict,[76] especially one in which we hold a developmental advantage. In any case, banning or limiting the weapons of IW would not affect the non-state actors, such as terrorists or criminal organizations, who may be our greatest near-term threat. Such bans would not eliminate the need for defensive measures. Rather they would increase the need for an offensive capability to counter the existing threat.

COMPLACENCY

A final option may be to accept the status quo and do nothing, or very little. As mentioned, currently international law does not conclusively address the legality of many forms of IW, or the appropriate responses to them. The potential and threat of IW has not yet reached a critical level because the attacks to date have not been particularly serious, in terms of damage or destruction.

However, as technology increases, the danger of a destructive attack seems likely. When its target is a U.S. system, we will undoubtedly respond. At this point, international law will be forced to address the issue of IW. It is obviously to our advantage to address the legal issues in advance, rather than being forced to address them in the midst of an emergency.

CONCLUSION

It is unlikely the international legal community will soon generate a comprehensive, coherent body of IW law. If the international legal community eventually deals with the issue and is able to develop a coherent set of guidelines, it is imperative that the U.S. realize law is not a panacea. Law itself will not guarantee the safety of U.S. systems or clearly define our offensive options. Law can help regulate national and individual behavior; it can critically aid our diplomatic efforts to alleviate or avoid conflict.

The speed of technological advancement far surpasses that of the legal system. It is quite plausible that advances in IW self-defense technology may be the only remedy to our current concerns. In this case, legal measures, over time, may merely supplement, not supplant preparedness.

There appears to be little reason why the U.S. should support negotiations in most areas of international law relevant to IW.[77] The principal exception is cooperation in apprehending international criminals; such efforts seek to improve mutual legal assistance.

There are currently no "show-stoppers" in international law that limit our efforts in the Department of Defense.[78] There are, however, many areas where legal uncertainties can create significant risk, which can be reduced by prudent planning.

WORD COUNT = 5936

ENDNOTES

[1] Bradley Graham, "Military Grappling with Guidelines for Cyber Warfare; Questions Prevented Use on Yugoslavia," The Washington Post, 8 November 1999, sec. 1A, p. 6.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Martin C. Libicki, What is Information Warfare? (Washington, D.C.: National Defense University), 1995, 7.

[6] Ibid.

[7] Louis Henkin, International Law: Politics and Values (1995), 38-39; quoted in Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law (Washington, D.C.: National Defense University Press, 1998), Chapter 1, 2.

[8] David J. DiCenso, "IW Cyberlaw: The Legal Issues of Information Warfare," Airpower Journal vol. XII, no. 2 Summer 1999): 92.

[9] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law (Washington, D.C.: National Defense University Press, 1998), Chapter 1, 3.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] International Court of Justice, "Legality of the Threat or Use of Nuclear Weapons," Advisory Opinion, para. 21; available from http://www.icj-cij.org/icjwww/idecisions/isummaries/iunanaummary960708.html; Internet; accessed 4 January 2001.

[15] Greenberg, Chapter2, 1.

[16] Gerd D. Wallenstein, International Telecommunications Agreements (1986), 67-69; quoted in Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law (Washington, D. C.: National Defense University Press, 1998), Chapter 2, 1.

[17] International Telecommunications Convention (hereinafter "ITC"), 1934, Article 35; available from google.com,

http://www.austlii.edu.au/au/other/dfat/treaties/1934/10.html+International+Telecommunications+Convention; Internet; accessed 4 January 2001.

[18] Greenberg, 1.

[19] Ibid.

[20] Ibid.

[21] Sean P. Kanuck, "Information Warfare: New Challenges for Public International Law," Harvard International Law Journal 37 (Winter 1996): 289.

[22] Greenberg, 3.

[23] Hague Convention (V) (hereinafter "Hague V"), "Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land," 18 October 1907; available from http://www1.umn.edu/humanrts/peace/docs/con5.html; Internet; accessed 4 January 2001.

[24] Greenberg, 3.

[25] Michael J. Robbat, "Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework and the Creation of a New Paradigm," Boston University Journal of Science and Technology Law (Spring 2000): 8.

[26] Hague V, Article 8.

[27] Robbat, 8.

[28] Department of Defense, Office of General Counsel, An Assessment of International Legal Issues in Information Operations (Washington, D.C.: Department of Defense, 2d edition, November 1999), 9.

[29] Hague Convention (IV) (hereinafter "Hague IV"), "Respecting the Laws and Customs of War on Land," 1907; Advisory Opinion 81; available from http://library.byu.edu/~rdh/wwi/hague/hague5.html; Internet; accessed 29 January 2001.

[30] Hague IV, Advisory Opinion 86.

[31] Greenberg, 4.

[32] Karl Kuschner, Major, USAF, "Legal and Practical Constraints on Information Warfare," available from http://www.airpower.maxwell.af.mil/airchronicles/cc/kuschner.html; Internet; accessed 20 October 2000.

[33] Robbat, 7.

[34] Ibid., 8.

[35] Ibid.

[36] DoD, Office of General Counsel, 39.

[37] Ibid.

[38] Ibid., 11.

[39] Gary H. Anthes, "New Laws Sought for Information Warfare as Technology Outpaces the Law," Computerworld, 5 June 1995, 1.

[40] Greenberg, 7.

[41] DoD, Office of General Counsel, 11.

[42] Ibid.

[43] U.N. Charter, Art. 51, Chap VII; available from http://www.un.org/aboutun/charter; Internet; accessed 4 January 2001.

[44] Robbat, 7.

[45] Ibid.

[46] U.N. Charter, Art. 51.

[47] Robbat, 7.

[48] Ibid.

[49] Ibid.

[50] U.N. Charter, Art. 51.

[51] Greenberg, 11.

[52] Ibid.

[53] U.N. Charter, Art. 39.

[54] U.N. Charter, Art. 41-49.

[55] Greenberg, 11.

[56] Ibid., Chapter 3, 1.

[57] Ibid., 2.

[58] Ibid.

[59] Mark W. Janis, An Introduction to International Law (2d edit., 1993), 1; quoted in Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law (Washington, D.C.: National Defense University Press, 1998), Chapter 3, 3.

[60] Greenberg, 3.

[61] United Nations, "United Nations Manual on the Prevention and Control of Computer-Related Crime," 264; available from http://www.sgrm.com/art25.html; Internet; accessed 3 February 2001.

[62] General Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Washington, D.C.: U.S. General Accounting Office, 22 May 1996), 22.

[63] Greenberg, 4.

[64] Ibid.

[65] Ibid.

[66] U.N. Charter, Art. 51.

[67] Greenberg, 8.

[68] Ibid., 9.

[69] Ibid.

[70] Marian L. Nash, Digest of United States Practice in International Law (Washington, D.C.: Office of the Legal Advisor, Department of State, 1983), 1749-1752.

[71] Greenberg, Chapter 4, 1.

[72] Ibid.

[73] Ibid., 2.

[74] Ibid.

[75] Ibid.

[76] Ibid., 3.

[77] "U.S. Military Grapples With Cyber Warfare Rules," Reuters, 8 November 1999; available from http://www.infowar.com/mil_c4i/99/mil_c4i_110899b_j.shtml; Internet; accessed 25 August 2000.

[78] DoD, Office of General Counsel, 47.

BIBLIOGRAPHY

Anthes, Gary H. "New Laws Sought for Information Warfare as Technology Outpaces the Law." Computerworld, 5 June 1995, 1-4.

DiCenso, David J., Major (Ret), USAF. "IW Cyberlaw: The Legal Issues of Information Warfare." Airpower Journal vol. XIII, no. 2 (Summer 1999): 85-102.

Graham, Bradley. "Military Grappling with Guidelines for Cyber Warfare; Questions Prevented Use on Yugoslavia." The Washington Post, 8 November 1999, sec. 1A, p. 6.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. Information Warfare and International Law. Washington, D.C.: National Defense University Press, 1998.

Hague Convention (IV). "Respecting the Laws and Customs of War on Land." 1907. Available from http://library.byu.edu/~rdh/wwi/hague/hague5.html. Internet. Accessed 29 January 2001.

Hague Convention (V). "Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land." 18 October 1907. Available from http://www1.umn.edu/humanrts/peace/docs/con5.html. Internet. Accessed 4 January 2001.

Henkin, Louis International Law: Politics and Values. 1995, 38-39. Quoted in Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law, Chapter 2, 2. Washington, D.C.: National Defense University Press, 1998.

International Court of Justice. "Legality of the Threat or Use of Nuclear Weapons," Advisory Opinion, 8 July 1996. Available from http://www.icj-cij.org/icjwww/idecisions/isummaries/iunanaummary960708.html. Internet. Accessed 4 January 2001.

International Telecommunications Convention, 1934. Available from google.com, http://www.austlii.edu.au/au/other/dfat/treaties/1934/10.html+International+Telecommunications+Convention. Internet. Accessed 4 January 2001.

Janis, Mark W. An Introduction to International Law. 2d edition, 1. Quoted in Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law, Chapter 3, 3. Washington, D.C.: National Defense University Press, 1998.

Kanuck, Sean P. "Information Warfare: New Challenges for Public International Law." Harvard International Law Journal 37 (Winter 1996): 272-292.

Kuschner, Karl, Major, USAF. "Legal and Practical Constraints on Information Warfare." Available from http://www.airpower.maxwell.af.mil/airchronicles/cc/kuschner.html. Internet. Accessed 20 October 2000.

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

Nash, Marian L. Digest of United States Practice in International Law. Washington, D.C.: Office of the Legal Advisor, Department of State, 1983.

Robbat, Michael J. "Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm." Boston University Journal of Science and Technology Law, Spring 2000 (10165 words). Database on-line. Available from Lexis-Nexis, Reed Elsevier.

U.N. Charter, "Article 51, Chapter VII." Available from http://www.un.org/aboutun/charter. Internet. Accessed 4 January 2001.

U.N. Manual, "United Nations Manual on the Prevention and Control of Computer-Related Crime." Available from http://www.sgrm.com/art26.html. Internet. Accessed 3 February 2001.

U.S. Department of Defense, Office of General Counsel. An Assessment of International Legal Issues in Information Operations. Washington, D.C.: Department of Defense, 2d edition, November 1999.

U.S. General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington, D.C.: U.S. General Accounting Office, 22 May 1996.

"U.S. Military Grapples With Cyber Warfare Rules," Reuters, 8 November 1999. Available from http://www.infowar.com/mil_c4i/99/mil_c4i_110899b_j.shtml. Internet. Accessed 25 August 2000.

Wallenstein, Gerd D. International Telecommunications Agreements. 1986, 67-69. Quoted in Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law, Chapter 2, 1. Washington, D. C.: National Defense University Press, 1998.