AU/ACSC/0116/97–03

LAW OF ARMED CONFLICT AND INFORMATION WARFARE—HOW DOES THE RULE REGARDING REPRISALS APPLY TO AN INFORMATION WARFARE ATTACK?

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Major Daniel M. Vadnais

March 1997

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government or the Department of Defense.

Contents

Page

Preface

There can be no doubt about the importance of information warfare, both in the way we fight now and in the way we will fight our future battles. The Chairman of the Joint Chiefs of Staff has made information warfare a priority item, and the Services are pressing to establish doctrine and capabilities. Like any other means of imposing our will on others, we need to understand when, where, why, how and upon whom we may implement this capability. I do not pretend to know the answer to any of these questions, but I recognized a gap in the materials I have read on the subject, and that is the topic of this paper. I hope the reader will come away with an understanding not of the answer, but of the tremendous complexity of the question.

I would like to express my gratitude to Mr. Walter Phillips of the Air Force Judge Advocate General School for pointing me in the right direction to explore, and for giving me unfettered access to all his information warfare materials. I would also like to thank my Faculty Research Advisor, Major Andre Provancha, for his moral support as I worked through this complicated area.

Abstract

The question of how to characterize an information warfare attack, particularly what is known as a "hacker attack," has not been fully developed. It must be, though, in order to understand how a nation can respond to it. This paper explores applicable tenets of international law. It identifies various methods of engaging in the spectrum of activities known as information warfare, and then discusses the one that has been underexplored in the context of a military response. Finally, it addresses the applicability of the law of armed conflict to a "hacker attack."

Given that during wartime, almost any means of imposing one belligerent's will on another is legitimate, subject to the various tenets international law, the question that needs to be addressed is what range of activities is permissible during times other than war, when parties are not engaged in traditionally understood applications of "armed force."

The current body of international law seems to mitigate against including "hacking" in the definition of "armed force," the standard necessary for unilateral military armed reprisal actions. In that case, unless the initial attack rises to the level that would permit some action by the "victim" in self–defense, that nation is relegated to seeking action from the United Nations Security Council.

Chapter 1

Introduction

> *Human history becomes more and more a race between education and catastrophe.*
>
> — H.G. Wells

Information warfare is charting new territory and creating new methods of imposing one's will on others. Compounding the problem is the nature of the post–Cold War world order, with non–traditional bodies (such as terrorist groups or contending factions within nation–states or even individual private citizens) playing significant roles in world politics. As technological innovations shape doctrine, strategies and tactics, the rules for using those innovative technologies must keep pace. Rules of Engagement need to be developed, taking into consideration applicable law of armed conflict rules and principles. Moreover, international law must adapt, too, taking into account information warfare methods of violating sovereignty without using traditionally–defined "armed force," but which methods in some cases may be just as effective.

Chapter 2

The Question

> *Nations nearly always go into an armed contest with the equipment and methods of a former war. Victory always comes to that country which has made a proper estimate of the equipment and methods that can be used in modern ways.*
>
> —William "Billy" Mitchell

In this "Third Wave" world[1], national (or individual or terrorist group, for that matter) efforts to impose one's will on another are not limited to the traditional political/diplomatic/economic/military instruments of power, but include the use of, or denial to another the use of, information. Much has been written about the proper characterization and the legality of information warfare, and limitations and restrictions on its use. An underexplored issue, though, is whether an armed response to an information warfare attack, whether that information warfare attack was legal or not, is permissible.

Since the establishment of the United Nations, wars of aggression have been outlawed.[2] This has resulted in two important developments: First, nations do not label their use of armed force as "war," and second, they rely on an official condonation of their armed action, either under the rubric of "self–defense," sanctioned by Article 51 of the United Nations Charter, or with the blessing of the United Nations Security Council under Chapter VII, Articles 39 and 42. The authors of those provisions did not address hostile efforts by a party to impose its will on another without using "armed force."

One key law of armed conflict consideration in information warfare is the rule regarding reprisals. Reprisals are permitted in international law when a belligerent violates international law during peacetime, or the law of armed conflict during wartime. If a foreign power is detected conducting information warfare operations that threaten to harm United States national capabilities or degrade the United States' defense posture, what types of responses might be appropriate? Would the use of deadly force be justified, even if an action caused no physical destructive effect and no personal injury? Would it make a difference whether the belligerent was engaged in physical hostilities with the United States at the time? Would it matter if the belligerent was not a traditionally–defined nation–state, but instead a terrorist group?

The questions relating to how information warfare may be used and regulated are abundant, ranging from the parties to a conflict (such as when an individual becomes a combatant, or how routing of information used to destroy or damage a military objective through a neutral country affects that country's neutrality), to the growing interdependence between the military and civilian society (including how the reliance of the military on civilian information resources mandates military protection of those resources, or how civilian reliance on military information resources affects the military's freedom to use or deny those resources). This paper focuses only on responses to non–lethal information warfare attack, specifically whether lethal force could be a legal response to such an attack. It addresses whether a non–lethal information warfare attack is a "use of force" which may be returned, or merely an act violative of international law, subject only to judicial recourse.

Notes

[1] Alvin Toffler, *The Third Wave* (New York: William Morrow & Co., Inc., 1980), 26. In this book, Toffler first discussed the idea that we are undergoing a third wave of change, following the First (the agricultural revolution) and the Second (the industrial civilization). The theme of that book is that this new wave is characterized by being highly technological and anti–industrial. *See also*, Alvin Toffler and Heidi Toffler, *War and Anti–War* (Boston: Little, Brown & Co., 1993), which explores the impact of this Third Wave, characterized in this latter book as the Information Age.

[2] United Nations Charter, Article 2(4) prohibits the use or the threat of force in international relations.

Chapter 3

The Law of Armed Conflict

> *We must not make a scarecrow of the law, setting it up to fear the birds of prey, and let it keep one shape, till custom make it their perch and not their terror.*
>
> —William Shakespeare

Foundations of the Law of War/Law of Armed Conflict

Principles and rules regulating armed hostilities between states was traditionally referred to as the law of war. Since the United Nations Charter effectively outlawed "war," the term "law of armed conflict" has been preferred instead. Multilateral conventions since the formation of the United Nations refer to "armed conflict" instead of "war."[1]

International law is "the standard of conduct, at a given time, for states and other entities subject thereto. It comprises the rights, privileges, powers, and immunities of states and entities invoking its provisions, as well as the correlative fundamental duties, absence of rights, liabilities and disabilities. International law, is, more or less, in a continual state of change and development."[2] It is also often a vague body of law, a concept not as foreign to some parts of the world as it seems to be to Western societies, where the rule of law is firmly entrenched.

The law of armed conflict is that part of the international law regulating parties in the conduct of armed hostilities.[3] The law of armed conflict exists to diminish the effects of conflict, to prevent unnecessary suffering, to safeguard fundamental rights, to prevent degeneration of conflict into savagery or brutality, and to facilitate the restoration of peace. "It has been said to represent in some measure minimum standards of civilization."[4] Compliance with the law of armed conflict reduces breakdowns in discipline, preserves resources (by not using them for investigating violations), and avoids world–wide outrage.[5]

It is well accepted that the law of armed conflict applies to an international armed conflict regardless of whether a state of "war" has been declared; indeed, "the international community has encouraged broad application of the law of armed conflict to as many situations as possible to protect the victims of conflicts."[6] The question of whether an information warfare "attack" constitutes force and therefore invokes the law of armed conflict is addressed *infra*.

The law of armed conflict is not a single treatise, but rather a compendium of agreements and understandings. "The law of war is to be found not only in treaties, but in the customs and practices of states which gradually obtained universal recognition, and from the general principles of justice applied by jurists and practiced by military courts. This law is not static, but by continual adaptation follows the needs of a changing world."[7] Treaty law, on the other hand, is merely contract law writ large. Like contract law, though, it binds only those parties who consent to be so bound, at least so far as the terms of the contract, or treaty, are beyond the scope of customary international law. On occasion, though, a treaty is so widely accepted in the international community that it can

be considered customary international law. Much of the customary law has been codified, in a number of conferences at The Hague in the Netherlands and Geneva, Switzerland.

The Hague Laws of 1907 generally dealt with the application of armed force. The basic principles of this body of law are those of military necessity, proportionality, humanity and chivalry. The principles of military necessity and humanity are actually the converse of each other: The former requires that force may only be applied to the degree required to accomplish one's military objectives at the least cost of life and physical resources. The latter prohibits the use of force or weapons not necessary for the purposes of war. The principle of proportionality combines the two, recognizing that collateral, non–military, damage will occur, but must not exceed the concrete military benefit attained. Chivalry refers to individuals' conduct and addresses such matters as truces and prisoners.

The 1949 Geneva Conventions generally define protection of combatants and noncombatants in four separate conventions (Wounded and Sick; Wounded, Sick and Shipwrecked; Prisoners of War; and Civilians). Additional protocols in 1977, not yet ratified by the United States, address international conflicts and non–international (domestic) conflicts.

International law affecting a state's military use of information or its denial of the use by others of information is scarce. But that does not mean concepts cannot be formulated and presented as proposals for establishing appropriate rules. The law of war has always had to deal with new weapons beyond the scope of existing law, though almost exclusively involving the use of armed force (the possible exception being reconnaissance satellites, which could arguably have been considered a weapon, although they are not so

considered now). In a sense, technological advances alter the future, while laws attempt to regulate the past. Clearly the law of armed conflict applies to air operations during armed conflict, yet when aircraft were first used in combat, there was no international convention nor any customary law regulating their use. The law, therefore, had to be extrapolated from other sources.

There are limitations regarding the access to free transmission of electronic data, including provisions of the International Telecommunications Satellite Organization and the International Maritime Satellite Organization (each of which limit the military or wartime use of their satellite systems), the Malaga Convention of 1973 and the Nairobi Convention of 1982 (restricting hostile interference with any member's radio communications), and domestic United States law.[8]

Basic Principles of the Law of Armed Conflict

AFP 110–31 defines the basic principles of military necessity, humanity, and chivalry:

> [Military necessity] justifies the use of regulated force not forbidden by international law which is indispensable for securing the prompt submission of the enemy, with the least possible expenditures of economic and human resources. The concept has four basic elements: (1) that the force used is capable of being and is in fact regulated by the user; (ii) that the use of force is necessary to achieve as quickly as possible the partial or complete submission of the adversary; (iii) that the force used is no greater in effect on the enemy's personnel or property than needed to achieve his prompt submission (economy of force); and (iv) that the force used is not otherwise prohibited.[9]

> Complementing the principle of necessity and implicitly contained within it is the principle of humanity which forbids the infliction of suffering, injury or destruction not actually necessary for the accomplishment of legitimate military purposes. This principle of humanity results in a specific prohibition against unnecessary suffering [and] a requirement of proportionality.[10]

> Although difficult to define, chivalry refers to the conduct of armed conflict in accord with well–recognized formalities and courtesies . . . . The principle of chivalry makes armed conflict less savage and more civilized for the individual combatant.[11]

The principle of proportionality simply acknowledges that the armed force applied in any operation may result in physical destruction and personal injury/death to other than military targets, but requires that it be limited to the extent consistent with the military necessity of the attack. In other words, the injury inflicted must be proportional to the military advantage sought. "The right of belligerents to adopt a means of injuring the enemy is not unlimited."[12] This applies to information warfare as well; the problem is in measuring and regulating injury in this context.

The Principle of Reprisal

"Traditionally, the law of armed conflict permitted states to engage in short–term, roughly proportional, but not necessarily symmetrical, punitive actions for violations of particular rights. Their actions are known as 'reprisals' and could be taken in peacetime in response to a general violation of international law or in wartime in response to some violation of the law of war."[13] Note that the definition of a reprisal includes the use of armed force, but does not limit it to such force. Two international court decisions set out the requirements and limitations on this action. There must be a violation of international law, followed by a request from the injured party for redress. Force may not be used "except in cases of necessity," and reprisals must be "approximately of the same degree as the injury to which they are meant as an answer" (in other words, it must be proportional to the initial injury).[14] Reprisals are not, however, permissible against neutrals, nor against a state not held liable for the original violation.[15]

Protocol I Additional to the Geneva Conventions of 1977 (not in force for the United States), provides that "civilian objects shall not be the object of attack or reprisals," and that attacks "shall be limited strictly to military objectives."[16] The American Law Institute restates it thusly: "A State victim of a violation of an international obligation by another state may resort to countermeasures that might otherwise be unlawful, if such measures (a) are necessary to terminate the violation or prevent further violation, or to remedy the violation; and (b) are not out of proportion to the violation and the injury suffered."[17] This right is qualified though: "The threat or use of force in response to a violation of international law is subject to prohibitions on the threat or use of force in the United Nations Charter…"[18]

An unaddressed issue regarding reprisals is whether they are permissible against non–state actors, including both groups and individuals. Before addressing that question, we must first establish the definitions of a "belligerent" and a "combatant," who are subject to and protected by the law of armed conflict, and subject to reprisals for violations of the law of armed conflict.

The Hague Convention defines a belligerent as an army, militia or volunteer corps fulfilling four conditions: they are commanded by a person responsible for his subordinates; they have a fixed distinctive emblem recognizable at a distance; they carry arms openly; and they conduct their operations in accordance with the laws and customs of war.[19] The law of armed conflict recognizes several different categories of actors. Combatants are persons who engage in hostile acts in an armed conflict on behalf of a party to the conflict. Lawful combatants may be regular forces, militia, or a "levee en masse," a spontaneous uprising by a state's population to resist invading armed forces. In

any case, though, to be a lawful combatant one must meet the four requirements stated above.

The law of armed conflict draws a clear distinction between combatants and noncombatants, for a variety of reasons. Primary among them is the protection of civilian noncombatants, by enabling a belligerent to distinguish between enemy belligerents and civilian noncombatants. The distinction also allows for execution of other law of armed conflict matters, such as surrender, treatment of prisoners of war, protection of the sick and wounded, and protection of protected sites.

When a combatant engages in acts during war that would be criminal during peacetime, he is not held criminally responsible for those acts (although he may be captured and detained as a POW for the duration of the conflict). He is protected by and because of his status. Conversely, when that person is not a combatant, and engages in those otherwise illegal acts, he is subject to criminal prosecution, not only for the underlying criminal act, but for engaging in combat as an unlawful combatant.

Until relatively recently, non–state actors did not often independently cross international boundaries to conduct acts in violation of international law (the primary exception being insurgents trained by neighboring states and striking across the frontier). But more importantly, the ability to take reprisal action against such an actor, if determined to be a lawful combatant, was constrained by one of the principles of the law of armed conflict, necessity. Recall that the principle of necessity requires that an armed attack against an enemy must be limited to its military objective. When the objective is a small group or an individual, and not a state, it becomes very difficult to strike just that offending target without at the same time injuring completely innocent citizens of the

"host" state. In the past, states have instead engaged in reprisals against the state supporting non–state actors, whether those actors were lawful or unlawful combatants. But such actions are not reprisals for the non–state actors' violation of international law, rather they are reprisals against the host state's violation, for intentionally providing support to the criminal. With the advances in precision munitions, and with the ability of a state to impose its will using hacker warfare, the matter of precision may no longer be a problem, and reprisals may be more likely in the future.

Nevertheless, it has been observed that the United States 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."[20] In other words, the United States may be disinclined to characterize an armed response as a reprisal, and instead label it an act of self–defense. More recently, former–President Bush stated that "Using our military force makes sense as a policy where the stakes warrant, where and when force can be effective, where no other policies are likely to prove effective, where its application can be limited in scope and time, and where the potential benefits justify the potential costs and sacrifice."[21]

Notes

[1] Article 2 of all four 1949 Geneva Conventions use this language: "The present Convention shall apply to all cases of declared war or of any other armed conflict which may arise…"

[2] Marjorie Millace Whiteman, *Digest of International Law* (Washington D.C.: Department of State, 1963), vol 1, 1.

[3] JCS Pub 1–02, *DoD Dictionary of Military and Associated Terms,* 23 March 1994. *See also generally* Marjorie Millace Whiteman, *Digest of International Law* (Washington D.C.: Department of State, 1963), vol. 10, chaps. 29 & 30.

[4] AFPD 51–4, *Compliance with the Law of Armed Conflict*, 26 April 1993, para 1–1.

Notes

[5] *Id*.

[6] AFP 110–31, *International Law—The Conduct of Armed Conflict and Air Operations*, 19 November 1976, 1–10.

[7] 1 *Trial of the Major War Criminals Before the International Military Tribunal, Nuremberg, 14 November 1945–1 October 1946* (Nuremberg, Ger., 1947), 221.

[8] 47 U.S.C. 502 provides criminal sanctions for "any person who willfully and knowingly violates . . . any rule, regulation, restriction, or condition made or imposed by any international radio or wire communications treaty or convention . . . ." 18 U.S.C. 1367 provides criminal sanctions for "whoever, without the authority of a satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite tranmission…"

[9] AFP 110–31, at 1–5, 1–6.

[10] AFP 110–31, at 1–6.

[11] AFP 110–31, at 1–6.

[12] Article 22, 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land.

[13] W. Michael Reisman and Chris T. Antoniou, *The Laws of War* (New York: Vintage Books, 1991), 23.

[14] Reisman & Antoniou, at 24, citing *Portugal v. Germany, Annual Digest of Public International Law Cases Years 1927 and 1928*, 526, Special Arbitral Tribunal, 31 Jul 28 (Meuron, Fazy, Guex.).

[15] *Portugal v. Germany, Annual Digest of Public International Law Cases Years 1929 and 1930*, 487, 30 Jun 30 (Meuron, Fazy, Guex.).

[16] Protocol Additional to the Geneva Conventions of 1949, Relating to Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N. Treaty Series 3, 27.

[17] *Restatement (Third) of Foreign Relations Law of the United States* (American Law Institute, 1987), Section 905.

[18] *Id*.

[19] 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land, Chapter I, Article 1.

[20] Marian L. Nash, *Digest of United States Practice in International Law 1979*,(Washington D.C.: Office of the Legal Advisor, Department of State, 1983), 1749–1752.

[21] "Bush's Talk to Cadets: When Force Makes Sense," *The New York Times*, 6 January 1993, A6.

Chapter 4

Information Warfare

If, then, civilized peoples do not put prisoners to death or sack cities and lay countries to waste, it is because intelligence plays a greater part in their conduct of war and has taught them more effective ways of applying force than these crude manifestations of instinct.

—Carl von Clausewitz

Definition of Information Warfare

Information warfare is defined by the Chairman of the Joint Chiefs of Staff as "Actions taken to achieve information superiority by affecting adversary information, information–based processes, and information systems while defending one's own information, information–based processes, and information systems."[1] It is "an amalgam of warfighting capabilities integrated into a CINC's theater campaign strategy and applied across the range of military operations and all levels of war."[2] The Air Force definition is similar: "Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[3]

To the United States military, information warfare is offensive and defensive actions taken to deny, exploit, corrupt or destroy the enemy's information and its functions, and to protect friendly and allied information systems from attack, while exploiting our own

military information functions. But there are as many more definitions of information warfare as there are writers who discuss it (*e.g.*, "information–age warfare" distinguished from "information warfare;"[4] "an electronic conflict in which information is a strategic asset worthy of conquest or destruction;"[5] or "distinct from 'computer crime' because it implies an aggressive act on the part of one adversary—whether an individual, a competing organization or a rival government—against another in an ongoing struggle for hegemony in the marketplace or the political arena."[6]). Martin Libicki, in his book, *What is Information Warfare*?, perhaps best characterizes it as not a single method of waging war, but several:

> Seven forms of information warfare—conflicts that involve the protection, manipulation, degradation, and denial of information—can be distinguished: (i) command–and–control warfare (which strikes against the enemy's head and neck), (ii) intelligence–based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace), (iii) electronic warfare (radio–electronic or cryptographic techniques), (iv) psychological warfare (in which information is used to change the minds of friends, neutrals, and foes), (v) "hacker" warfare (in which computer systems are attacked), (vi) economic information warfare (blocking information or channeling it to pursue economic dominance), and (vii) cyberwarfare (a grab bag of futuristic scenarios).[7]

Only Libicki's "hacker warfare" is the type this paper is concerned with, because that is the type of peacetime hostile use of the information "weapon" that will raise the question whether such use would justify a response using armed force. Nevertheless, there can be no doubt that information warfare of all types deserves careful study. Libicki notes that "As long as the power of information technology doubles every two or three years, it will continue to have a disproportionate effect on the evolution of national security.[8]

Is Information Warfare "The Use of Force" as Contemplated by the United Nations?

Article 2(4) of the United Nations Charter 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." However, Article 51 allows that "[n]othing 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," and Chapter VII, Articles 39 and 42 permit the United Nations Security Council to "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 taken in accordance with Articles 41 (regarding non–military responses) and 42, or to maintain or restore international peace and security." Article 42 states: "Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such actions by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such actions may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."

The definition of "use of force" from Article 2(4) has been addressed on several occasions, but never pinned down. Indeed, at the San Francisco Conference in 1945, proposals to define "aggression" were defeated, and it was decided instead to give the United Nations Security Council complete discretion to determine what constitutes a threat to or breach of the peace, or an act of aggression.[9] Again in 1970, the United Nations declined to define the term "use of force," at the time focusing on how to

characterize political or economic coercion.[10] However, neither the long–standing United States economic embargo against Cuba nor the 1973 Arab oil embargo has been considered in the international community as a "use of force."[11]

Establishing a definition of the term "use of force" is important to determine when a nation is authorized to unilaterally respond to a peacetime hacker attack, but the lack of a definition does not mean that a nation is powerless to respond. In the event of an information warfare attack that would not universally be described as "use of force," a state would have to go to the United Nations Security Council for authorization to respond under Article 42.

Limitations of Information Warfare

Despite the doomsday characterization of the effects of information warfare, not all the experts are convinced of its invincibility nor of its ability to independently conquer a nation. Professor Libicki opines that "[i]n its ability to bring a country to its knees, hacker warfare is a pale shadow of economic warfare, itself of limited value. Suppose that hackers could shut down all phone service (and, with that, say, credit card purchases) nationwide for a week. The event would be disruptive certainly and costly (more so every year), but probably less disruptive than certain natural events, such as snow, flood, fire, or earthquake—indeed, far less so in terms of lost output than a modest–size recession."[12] He concludes his paper by asserting that "almost certainly there is *less* to information warfare than meets the eye [emphasis in original]."[13] Whether Professor Libicki's view is too optimistic or not, he raises a valid point, that information warfare is not, and it should not be analyzed in the same way as, a weapon of mass destruction.

Information Warfare as a Legitimate Weapon

During a state of declared or acknowledged hostilities, any means, within the strictures of the law of armed conflict, are legitimate for the purpose of attaining a state's objectives. In the absence of declared or acknowledged armed hostilities, the permissible use of hacker warfare is unaddressed by current doctrine.

While there is no official joint or Air Force doctrine on the employment of that part of information warfare that is the subject of this study, current thinking holds that information warfare is simply another tool in a warfighter's toolbox.[14] Like any other tool, information warfare weapons must be used consistently with the law of armed conflict. The Air Force policy is clear: "Air Force personnel will comply with [the law of armed conflict] in military operations and related activities *during armed conflicts*, no matter how these conflicts are characterized [emphasis added]."[15] The Air Force then defines "armed conflict": "A conflict between states in which at least one has resorted to using armed force to achieve its aims."[16]

Weapons are defined as: "Devices designed to kill, injure or disable people, or to damage or destroy property. The following are not weapons: Devices developed and used for training and practice; aircraft, intercontinental ballistic missiles, and other launch platforms; and *electronic–warfare devices* [emphasis added]."[17] Webster's dictionary gives a different spin, defining a weapon as "an instrument of offensive or defensive combat used in destroying, defeating or physically injuring an enemy."[18]

There seems to be a discordance between the Air Force's exclusion of the information warfare spectrum from the definition of a weapon and the Air Force's current doctrine espousing the criticality of all the various means of offensive information warfare in

wartime.[19] The proper resolution is to acknowledge that information warfare systems can be just as effective in imposing a nation's will as traditional firepower, so should be included in the definition of a weapon and should be subject to legal review of their intended employment.

Notes

[1] CJCSI 3210 DRAFT, para. 4c, as of 6 Oct 95.

[2] *Information Warfare: A Strategy for Peace… The Decisive Edge in War*, JCS Publication, 2.

[3] *Cornerstones of Information Warfare*, SAF/CSAF Publication, 3–4.

[4] Maj Richard W. Aldrich, "The International Legal Implications of Information Warfare," *Airpower Journal*, Fall 1996, 101.

[5] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), 13.

[6] Richard Power, *Current and Future Danger: A CSI Primer on Security Crime and Information Warfare*, (San Francisco: Computer Security Institute, 1995).

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

[8] Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (Washington, D.C.: National Defense University, 1995), 161.

[9] Doc. 943, III/5, 11 U.N.C.I.O. Doc. 17 and 12 U.N.C.I.O. Doc. 505, collected at Clyde Eagleton, ed., *Annual Review of United Nations Affairs* (New York: New York University Press, 1945).

[10] *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations*, U.N. General Assembly Official Records, 25th Sess., U.N. Doc. A/RES/2625 (1970). *See also*, Robert Rosenstock, "The Declaration of Principles of International Law Concerning Friendly Relations: A Survey," 65 Am. J. Int'l L. 713, 720 (1971).

[11] See Jordan J. Paust and Albert P. Blaustein, "The Arab Oil Weapon—A Threat to International Peace," 68 Am. J. Int'l L. 410 (1974); Ibrahim F.I. Shihata, "Destination Embargo of Arab Oil: Its Legality Under International Law," 68 Am. J. Int'l L. 591 (1974); and Tom L. Farer, "Political and Economic Coercion in Contemporary International Law," 79 Am. J. Int'l L. 405 (1985).

[12] Martin C. Libicki, *What is Information Warfare?* (Washington D.C.: National Defense University Press, 1995), 60.

[13] *Id*. at 96.

[14]*Information Warfare: A Strategy for Peace . . . The Decisive Edge in War*, JCS Publication.; *Cornerstones of Information Warfare*, SAF/CSAF Publication.

[15] AFPD 51–4, *Compliance with the Law of Armed Conflict*, 26 April 1993, para. 1.2; AFI 51–401, *Training and Reporting to Ensure Compliance with the Law of Armed Conflict*, 19 July 1994, para.1.1.

Notes

[16] AFPD 51–4, para. 1.6.1.

[17] AFPD 51–4, para. 1.6.5; AFI 51–402, *Weapons Review*, 13 May 1994, para. 1.

[18] *Webster's Third New International Dictionary of the English Language, Unabridged* (Springfield, Massachusetts: G.&C. Merriam Co., 1986).

[19] *Information Warfare: A Strategy for Peace . . . The Decisive Edge in War*, JCS Publication, 14.

Chapter 5

The Law of Armed Conflict and Information Warfare

> *A new set of rules for the conduct of war will have to be devised and a whole new set of ideas of strategy learned by those charged with the conduct of war.*
>
> — William "Billy" Mitchell

Does the Law of Armed Conflict Apply To Information Warfare?

The drawback to a nation of holding that information warfare techniques are equivalent to armed force, and subject to the law of armed conflict, is the restrictions they then impose on their own use of those same techniques. A nation that has the capability to engage in hacker warfare is disinclined to regulate its own use of that instrument at the risk of suffering another nation's exploitation of it. It would always be to the advantage of the more technologically advanced nation to have hacking *not* be considered a use of "armed force," with the onus and the restrictions that accompany that characterization. As other actors (nations, terrorist groups, individuals) attain the same level of technological sophistication, though, it becomes more advantageous to characterize some uses as "armed force" or the equivalent thereof, in order to reduce the chances of becoming the victim, or to legitimize an armed response to an information warfare attack. That seems to be the situation now.

The law of armed conflict is "[t]hat part of international law that regulates the conduct of armed hostilities."[1] To the extent that information warfare can be characterized as armed force, the rules of the law of armed conflict clearly apply. Also, there are international treaties that would restrict information warfare capabilities, such as the International Telecommunications Satellite and International Maritime Satellite Organizations, and the Malaga and Nairobi Conventions discussed in Chapter 3, *supra*.

If a nation determined that an information warfare attack upon it was in fact an act of "armed force" and decided to respond with armed force, then obviously the Laws of Armed Conflict would apply. The unsettled issue, though, is *when* information warfare can or should be so characterized. A logical answer is that an information warfare attack that results in the same sort of damage or injury that armed force would inflict should be considered equivalent to armed force. This would distinguish a hacker attack that results in death, such as an interruption or manipulation of data resulting in a medical facility shutting down or an airliner crashing, from an embargo, which is not considered to be a use of force despite its long–range potential for lethal effect.

Chairman of the Joint Chiefs of Staff Instruction 3210 recognizes that the capabilities of many information warfare systems make them weapon systems that may be used during armed conflict. On the other hand, Air Force Policy Directives and Instructions explicitly exclude some information warfare capabilities from their definition of "weapons." So to a large extent, it is a matter of definition—what is often called "information warfare" is actually a number of capabilities, some old, some new. Some seem clearly to be equivalent to "armed force," such as electronic warfare actions like jamming enemy radar, or Command and Control Warfare. Used during or immediately prior to engaging in

traditional "armed force" applications, such uses of the information realm should be so considered. Others seem clearly to not be "armed force," such as Libicki's "economic information warfare," just as certainly as any other implementation of a nation's economic instrument of power is not the use of armed force. But those two examples are clear only because they take place normally during what can clearly be characterized as either a state of armed conflict or not. Electronic warfare means are normally implemented clandestinely, as part of an armed conflict operation. Economic means are implemented openly, often in concert with other non–military instruments of power.

A further consideration in the debate is the requirement that any weapon intended to meet a military requirement must undergo a legal review to ensure that its intended use is consistent with the domestic and international legal obligations of the United States. The exclusion of "electronic warfare devices" from such a review does not seem appropriate in light of the ever–expanding realm of electronic warfare.

If Clausewitz was correct, and war is simply one means of pursuing a state's political ends[2], then we should not assume that every act taken by another state that impacts ours is "armed conflict." Indeed, political, diplomatic and economic instruments of power are certainly not limited by the laws of armed conflict. However, we should not be blind to the potential uses of, and the potential military value of, these weapons.

Can Deadly Force Be A Proportional Reprisal For Information Warfare?

A reprisal is a short–term, roughly proportional, punitive response to a violation of international law. There are a myriad of potential responses to a hacker attack: If the attack violates specific international laws, a judicial remedy may lie. Alternatively, an

economic, diplomatic, political or corresponding information–related response would certainly be justified and could be the most effective means.

When a hacker attack results in effects identical to that of an armed attack, then the same consequences may be justified. If a nation wishes to consider a hacker attack as equivalent to an attack by armed force, then a unilateral reprisal or act of self–defense would be justified, as long as it was limited in scope to address the violation or threat. If, on the other hand, a nation does not wish to consider such an attack as one by armed force, then it could only respond by first implementing non–military instruments of power, and, if they are unsuccessful, by seeking United Nations action under Article 42 by arguing that the hacker attack was an act of aggression or a breach of the peace.

One must be careful to not fall under the spell of information warfare, though, and believe that it has mystical powers or that it is more powerful than any other instrument of power or implement of armed force. Nations and other actors will engage in attempts to impose their will on others when they see fit, by whatever means are at their disposal. It is, after all, simply the latest weapon in an ever–changing arsenal.

During wartime, deadly force may be used to accomplish any legitimate military objective, subject to the law of armed conflict principles of military necessity, proportionality, humanity and chivalry. An information warfare attack that violates law of armed conflict rules could be the subject of like reprisal, though. If an information warfare attack violates international law (most likely a treaty, since there is so little customary law applicable to the use of information), then an armed attack as a reprisal may be supportable, if it is similar in kind to the original wrong, and complies with the principles

of proportionality and humanity, but other recognized judicial and United Nations resolutions should first be sought.

Conclusion

We have defined the terms information warfare and Reprisals, and examined how they may be used. During wartime, armed force is limited only by the law of armed conflict principles of military necessity, proportionality, humanity and chivalry. During peacetime, armed force may only be used as a reprisal or when the United Nations sanctions it, normally only in self–defense. The term "armed force" was and is the subject of many debates in the international relations forum.

To the extent that information warfare is manifested by traditionally–understood damage to sovereign integrity, the law of armed conflict should apply, and proportional reprisals may be justified. On the other hand, to the extent that damage to a sovereign's integrity is not physical, there is a gap in the law. That gap should be closed.

Information warfare treaties have been proposed. It seems logical to consider them in light of this particular question. In the meantime, the United States armed forces would be well–served by a unilateral United States policy and Rules of Engagement regarding the use of information warfare, from both an offensive and defensive perspective.

Notes

[1] JCS Pub 1–02, *DOD Dictionary of Military and Associated Terms*, 23 March 1994.

[2] Carl von Clausewitz, *On War* (Princeton, New Jersey: Princeton Univ. Press, 1984), 88.

Bibliography

47 U.S.C. 502.

18 U.S.C. 1367.

AFI 51–401, *Training and Reporting to Ensure Compliance with the Law of Armed Conflict*, 19 July 1994.

AFI 51–402, *Weapons Review*, 13 May 1994.

AFP 110–31, *International Law—The Conduct of Armed Conflict and Air Operations*, 19 November 1976.

AFPD 51–4, *Compliance with the Law of Armed Conflict*, 26 April 1993.

Aldrich, Maj Richard W. "The International Legal Implications of Information Warfare," *Airpower Journal*, Fall 1996.

Article 22, 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land.

"Bush's Talk to Cadets: When Force Makes Sense," *The New York Times*, 6 January 1993.

CJCSI 3210 DRAFT, as of 6 Oct 95.

Clausewitz, Carl von. *On War* (Princeton, New Jersey: Princeton Univ. Press, 1984).

Cornerstones of Information Warfare, SAF/CSAF Publication.

Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, U.N. General Assembly Official Records, 25th Sess., U.N. Doc. A/RES/2625 (1970).

Eagleton, Clyde ed., *Annual Review of United Nations Affairs* (New York: New York University Press, 1945).

Farer, Tom L. "Political and Economic Coercion in Contemporary International Law," 79 Am. J. Int'l L. 405 (1985).

Information Warfare: A Strategy for Peace…The Decisive Edge in War, JCS Publication.

JCS Pub 1–02, *DOD Dictionary of Military and Associated Terms*, 23 March 1994.

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

Libicki, Martin C. *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (Washington, D.C.: National Defense University, 1995).

Nash, Marian L. *Digest of United States Practice in International Law 1979*, (Washington D.C.: Office of the Legal Advisor, Department of State, 1983).

Paust, Jordan J. and Albert P. Blaustein, "The Arab Oil Weapon—A Threat to International Peace," 68 Am. J. Int'l L. 410 (1974).

Portugal v. Germany, *Annual Digest of Public International Law Cases Years 1929 and 1930*, 30 Jun 30 (Meuron, Fazy, Guex.).

Protocol Additional to the Geneva Conventions of 1949, Relating to Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N. Treaty Series 3.

Reisman, W. Michael and Chris T. Antoniou, *The Laws of War* (New York: Vintage Books, 1991).

Restatement (Third) of Foreign Relations Law of the United States (American Law Institute, 1987).

Richard *Current and Future Danger: A CSI Primer on Security Crime and Information Warfare*, (San Francisco: Computer Security Institute, 1995).

Rosenstock, Robert. "The Declaration of Principles of International Law Concerning Friendly Relations: A Survey," 65 Am. J. Int'l L. 713 (1971).

Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994).

Shihata , Ibrahim F.I., "Destination Embargo of Arab Oil: Its Legality Under International Law," 68 Am. J. Int'l L. 591 (1974).

Toffler, Alvin. *The Third Wave* (New York: William Morrow & Co., Inc., 1980).

Toffler, Alvin and Heidi Toffler. *War and Anti–War* (Boston: Little, Brown & Co., 1993).

Trial of the Major War Criminals Before the International Military Tribunal, Nuremberg, 14 November 1945–1 October 1946 (Nuremberg, Ger., 1947).

Webster's Third New International Dictionary of the English Language, Unabridged (Springfield, Massachusetts: G.&C. Merriam Co., 1986).

Whiteman, Marjorie Millace *Digest of International Law* (Washington D.C.: Department of State, 1963), vols. 1, 10.