HOW DO YOU KNOW YOU ARE AT WAR IN THE INFORMATION AGE?

Lieutenant Colonel Richard W. Aldrich[*]

TABLE OF CONTENTS

[*]Deputy Staff Judge Advocate, Air Force Office of Special Investigations. B.S. (Computer Science), United States Air Force Academy, 1981; J.D., UCLA School of Law, 1986; LL.M., Intellectual Property, University of Houston Law Center, 1999. This paper was produced under a grant from the Institute for National Security Studies (INSS). The views expressed herein are those of the author and do not necessarily represent the views of the INSS, the United States Air Force, the Department of Defense, or any other officer or entity of the United States Government.

> *It is not at all clear at this time whether information-warfare measures taken by a potential adversary . . . would be readily detectable. The question of "how do you know you are at war" may be difficult to resolve in view of the potential ambiguity associated with Information Warfare.*[1]

I. INTRODUCTION

In earlier times the question, "How do you know you are at war?" would have seemed disingenuous. When the boulders came catapulting over the fortress wall, one could be fairly certain one was at war. Battering rams punching in the king's fortifications, rows of redcoats firing muskets in unison, and incoming cannonballs were all fairly clear indicators of war. Wars, at one time, were even formally declared, which of course took much of the guesswork out of it. But in recent times war has been become more difficult to define, and information warfare (IW) seems likely to be the most elusive yet.[2] Part of the reason is that IW can take place in an entirely new realm, that ethereal place some call "cyberspace"[3] and others call the "infosphere."[4] Another reason is that many of the weapons used can be bought in any computer store and look exactly like the tools used to produce term papers and generate spreadsheets. The weapons' effects may not be to produce immediate death and destruction of property, but to innocuously manipulate bits of data, changing ones to zeros and vice versa, to deleterious effect nonetheless. Finally, the objects of the attack are less

---

1. *The Revolution in Military Affairs* (visited Nov. 15, 1999) <http://www.armyec.sra.com/knowbase/docs/doc5/rmapaper.htm>.

2. *See* Reto E. Haeni, *An Introduction to Information Warfare* (visited Nov. 12, 1999) <http://tangle.seas.gwu.edu/~reto/infowar/info-war.html>.

3. *See* Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 JURIMETRICS J. 1, 3 (1994) (identifying William Gibson as the creator of the term "cyberspace," defined as "the virtual space created by the interconnection of computers").

4. *See* JAMES ADAMS, THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE 14 (1998) (defining infosphere as "the virtual world where commerce, conversation and connectivity will all occur").

likely to be traditional military targets, and more likely to be a nation's "commercial and industrial underpinnings," its telecommunications companies, power companies, financial centers, and the like.[5] Many believe that an "electronic Pearl Harbor" is inevitable.[6] This all requires a serious reevaluation of what constitutes an illegal use of force in the Information Age.[7]

The importance of delineating what constitutes a "use of force" in the age of IW[8] is twofold. First, it assists in determining when the United States may be entitled to exercise self-defense or some lesser form of sanctions against one who uses certain infowar techniques against the United States.[9] Second, it puts the United States on notice as to when its own conduct may legitimately be described as a use of force, thereby entitling other nations to take self-defense or other appropriate measures.[10] Currently there is a dearth of guidance on the issue. Indeed, one prominent practitioner has opined, "Currently, we are unable to reliably forecast what kinds of electronic attack would be considered by a target country or by the international community to be an 'act of war'."[11]

---

5. *The Nation at Risk: Report of the President's Commission on Critical Infrastructure Protection: Hearing Before the Subcomm. on Technology, Terrorism, and Gov't Information of the Senate Comm. on the Judiciary*, 105th Cong. 8–9 (1997) (statement of John J. Hamre, Deputy Secretary of Defense).

6. *Id.*

7. *See generally* ALVIN & HEIDI TOFFLER, WAR AND ANTI-WAR: SURVIVAL AT THE DAWN OF THE 21ST CENTURY (1993) (characterizing the Information Age as the Third Wave, reflecting their view that these epochs are fluid and less susceptible to characterizations which define clear boundaries, while the First and Second Waves referenced the agricultural and industrial ages respectively).

8. The Air Force defines information warfare as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions." Department of the Air Force, *Cornerstones of Information Warfare* (visited Nov. 18, 1999) <http://www.af.mil/lib/corner.html>.

9. Further, because the United States is a party to several collective self-defense treaties, the "use of force" also determines when the United States could come to the aid of another nation-state subjected to an information attack.

10. For the proposition that law does influence and constrain the conduct of governmental actors, even when vital security interests are at stake, see LOUIS HENKIN, HOW NATIONS BEHAVE: LAW AND FOREIGN POLICY 285–96 (2d ed. 1979).

11. Interview with CDR Jane G. Dalton, JAGC, USN, Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff (Feb. 18, 1998). CDR Dalton notes, however, that the question is largely academic in that "the

II. BACKGROUND

This Article will begin by discussing the vulnerability of military systems within the United States, and the vulnerability of the U.S. information infrastructure, upon which the military relies heavily. The Article will then discuss some recent "attacks" and how their level of sophistication has improved markedly. Finally, it will address issues in detecting attacks, as well as the costs associated with such attacks.

A. Scope of the Problem

While some still speak of IW as a futuristic concept posing only a potential concern for future generations, the fact is that information warfare under its broadest definition has probably always been a part of warfare.[12] Some definitions of information warfare include the conventional bombing of a computer center, as well as propaganda ploys designed to confuse the enemy.[13] While I do not contest the potential breadth of the term "information warfare," this paper will primarily focus more narrowly on those aspects of IW dealing with the use of information systems as offensive or defensive weapons. Conventional uses of force against information systems, such as the bombing of a computer center, can largely be dealt with using established law of armed conflict constructs to assess military necessity, proportionality, collateral damage, and the like.[14] It is the use of nontraditional information weapons which raise the most interesting questions under current law, and which will be the focus of this paper.

The threat of an information attack with serious military implications is very real.[15] For instance:

> A group of Dutch hackers calling themselves 'High Tech for Peace' approached diplomats in the Iraqi embassy in Paris. For a payment of $1 million,

---

threshold for an act to be considered an act of war is so high that the target nation's rights under international law could be violated long before reaching the level of an act of war." *Id.*

12. *See* Maj. Richard W. Aldrich, USAF, *The International Legal Implications of Information Warfare*, AIRPOWER J. 99, 99–101 (Fall 1996).

13. *See id.* at 100–02 (discussing various definitions of the term "information warfare").

14. *See id.* at 102.

15. *See generally* ADAMS, *supra* note 4.

> the Dutch hackers offered to foul up the network handling logistics messages between bases in the United States and U.S. military units in Saudi Arabia. The Iraqis rejected the idea.[16]

While it is not entirely clear what impact the Dutch hackers could have had on the Gulf War, the coalition's vulnerability was such that it may have been $1 million effectively spent.[17] Some twenty-five percent of the message traffic into Saudi Arabia during the Gulf War was "open, unencoded, [and] on the Internet."[18] Smart hackers would not have needed to debilitate the communications. Merely manipulating some of the communications could potentially have had a grave effect.[19] A few misdirected tanks and other armaments could have so foiled battle plans that all data would thereafter have become suspect, at least temporarily paralyzing operations.[20] This potential for disaster did not go unnoticed.

> In the wake of the 1991 Gulf War the Department of Defense, having comprehensively dismantled Iraq's critical infrastructures, began to express concern at the vulnerabilities of its own infrastructures. A series of studies and war games, along with the well-publicised activities of hackers, demonstrated that the U.S. armed forces had left themselves wide open to disruption of their command, control, communications and logistics infrastructures as a result of their rush to adopt digital, wide area information networks.[21]

How has the United States become so vulnerable? In large part, U.S. vulnerability to such attacks is a product of the fairly rapid computerization of America's businesses and military, and the even more revolutionary shift to large scale

---

16. JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA 104–05 (1997).

17. *See id.* at 105.

18. *Id.*

19. *See id.*; *see also* Captain Robert G. Hanseman, USAF, *The Realities and Legalities of Information Warfare*, 42 A.F.L. REV. 173, 193 (1997) (discussing information attack scenarios and the vulnerability of Pentagon computer networks).

20. *See* Hanseman, *supra* note 19, at 193.

21. Andrew Rathmell, *Information Warfare—USA Tackles Cyber Threat*, JANE'S INTELLIGENCE REV.-POINTER, Sept. 1, 1998, at 14, *available in* 1998 WL 789725.

networking of computers.[22] The military has 2.1 million computers and 10,000 local area networks (LANs).[23] These facts caused the authors of the Defense Science Board Report to observe, "We have built our economy and our military on a technology foundation that we do not control and, at least at the fine detail level, we do not understand."[24] Few probably were aware of the heavy dependence upon a single satellite for pager communications until Galaxy 4 spun out of control in May 1998, resulting in lost service to approximately 35 million users.[25] Also affected were, among others, National Public Radio and a large number of private corporate networks.[26]

1. Vulnerability of DOD Systems

How often and how seriously the Defense Department is subjected to information attacks is subject to widely varying reports.[27] One report claimed the military's computers are probed by outsiders about five hundred times a day.[28] The

---

22. *See* Neil Munro, *Sketching a National Information Warfare Defense Plan*, 39 COMMS. OF THE ACM 15, Nov. 1996, *available in* LEXIS, News Library, Magpap File. "[T]he nation's myraid of computer-controlled networks, the phone switches, the powergrid, the air-traffic control system, the banks, can all be wrecked during a war or crisis by hostile hackers funded and protected by countries such as Iran . . . ." *Id.*; *see also* George Leopold, *"Infowar": Can Bits Really Replace Bullets?*, ELEC. ENG'G. TIMES, Nov. 6, 1995, at 65 ("Global connectivity has heightened Pentagon concerns about information security and the need for adequate defenses."); M.J. Zuckerman, *Information Warfare: A Real Threat*, USA TODAY, Oct. 20, 1997, at 18A (showing that the U.S. military depends on public telephone networks for 95% of its computer networking).

23. *See* U.S. GENERAL ACCOUNTING OFFICE, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS, REP. NO. GAO/AIMD-96-84 (1996) (visited Nov. 10, 1999) <http://www.gao.gov> (statement of Jack L. Brock, Jr., Director, Defense Information and Financial Management Systems) [hereinafter GENERAL ACCOUNTING OFFICE].

24. Thomas E. Ricks, *Information–Warfare Defense is Urged: Pentagon Panel Warns of 'Electronic Pearl Harbor'*, WALL ST. J., Jan. 6, 1997, at B2.

25. *See* Arnaud de Borchgarve, *Hackers Probed in Failure of Satellite, International Group Has Made Threats*, WASH. TIMES, May 23, 1998, at A1.

26. *See* Seth Schiesel, *Millions Await Beep, But Box Remains Silent*, N.Y. TIMES, May 21, 1998, at A1.

27. *See* Timothy W. Maier, *Is U.S. Ready for Cyberwarfare?*, INSIGHT ON THE NEWS, April 5, 1999, at 18 (arguing that the General Accounting Office report of 250,000 incidents in 1995 is inflated; the Pentagon claims there were only 500 that year).

28. *See* Douglas Waller, *Onward Cyber Soldiers*, TIME, Aug. 21, 1995, at 38, 39. A CIA report concluded that even though there have been no clear attacks on the military's computer facilities, several foreign intelligence services have already probed U.S. computers. A Justice Department official claims that

same report indicates only about twenty-five percent of those intrusions were detected.[29] The General Accounting Office (GAO) reports about 250,000 suspected attacks occurred in 1995, with the number doubling each year.[30] Of those attacks, the GAO report stated sixty-five percent were successful.[31]

The military conducted a classified exercise in the summer of 1997, which ran under the code name Eligible Receiver, in an attempt to assess its vulnerability.[32] The purpose of the exercise was to show the ease with which the military's 2.1 million computers, 10,000 local area networks and 100 long-distance networks could be disabled.[33] In an ironic good news/bad news release, the exercise was deemed a success beyond its planners' wildest dreams, because the attack team was so easily able to penetrate Department of Defense (DOD) systems that it dramatically demonstrated continuing widespread vulner-ability.[34] Even before the exercise, "the government's Joint Security Commission called U.S. vulnerability to infowar 'the major security challenge of this decade and possibly the next century'."[35]

2. Level and Character of Attacks

Two California teens (using code names Makaveli and TooShort and operating under the direction of Ehud Tenebaum, a.k.a. The Analyzer, a hacker in Israel) were arrested after a concentrated series of break-ins to military computers.[36] The hackers hit hundreds of sites, including the

---

five of the last seven identified intruders to the Pentagon's mainframes were foreigners. *See id.*

29. *See id.*

30. *See* GENERAL ACCOUNTING OFFICE, *supra* note 23.

31. *See id*; *see also* Maier, *supra* note 27, at 18 (noting that one chief executive officer of a security company, who is also an expert forensic witness, claims that the 250,000 figure is not important, but that "65% of the hackers got in" is important).

32. *See* William Jackson, *DOD Set to Fight Hackers Both Foreign and Domestic*, GOV'T COMPUTER NEWS, Aug. 23, 1999, at 8, *available in* LEXIS, News Library, Mags File.

33. *See* Bob Drogin, *U.S. Scurries to Erect Cyber-Defenses*, L.A. TIMES, Oct. 31, 1999, at A1.

34. *See id.*

35. Waller, *supra* note 28, at 38.

36. *See* Dan Reed & David L. Wilson, *Suspected Pentagon Hacker Found—FBI Arrests Israeli Teen Who Had Bragged He Couldn't Be Caught*, SEATTLE TIMES, March 19, 1998, at A7.

Air Force and the Navy.[37] At the time the attack was called "the most organized and systematic attack to date."[38]

Just a couple of months later, the level was ratcheted up further when the Masters of Downloading (MOD), a group of older hackers revealed that they had broken into a sensitive Pentagon network in October of 1997.[39] MOD had allegedly stolen software which coordinated the military's Global Positioning System, a system of satellites "used to target missiles and . . . enable troops to pinpoint their positions."[40] Shortly after this revelation, MOD alleged that it had also stolen NASA computer programs.[41] In an Internet chat interview, MOD members indicated they were willing to sell the sensitive computer programs.[42]

3. Triggering an Appropriate Response

Defining precisely what constitutes a "threat or use of force" as that term is used in the U.N. Charter, and therefore what triggers the offended nation-state's right to respond, whether diplomatically or through the employment of self-defense measures under Article 51, is necessarily complex and not subject to simplistic tests.[43] Similar complexities surround what constitutes an act of aggression under Article 39.[44]

This is true whether one is evaluating suspected information attacks or more conventional kinetic attacks. Thus, this Article does not presume to set out a test that will yield a definitive black and white answer, but rather will address the factors that should go into evaluating such a

---

37. *See id.*

38. *Id.* (quoting a government official).

39. *See* Jim Doyle, *Cybergangs*, SAN FRANCISICO CHRON., April 27, 1998, at A19.

40. *Id.*

41. *See* John Bacon, *NASA Hacked*, USA TODAY, April 23, 1998, at 3A.

42. *See id.*

43. *See* Capt. Sean M. Condron, *Justification for Unilateral Action in Response to the Iraqi Threat: A Critical Analysis of Operation Desert Fox*, 161 MIL. L. REV. 115, 126 (1999) (stating that the limits of the self-defense provision have been a topic of debate since 1945); *see also* Thomas K. Plofchan, Jr., *Article 51: Limits on Self-Defense?*, 13 MICH. J. INT'L L. 336, 338–39 (1992) (using a two-prong analysis with distinct sub-parts to define "self-defense" under Article 51).

44. *See* Plofchan, *supra* note 43, at 344–45 (noting that Article 51 has been said to have phrasing similar to Articles 39, 41, and 42 when discussing how Article 51 should be interpreted).

determination, and the special complexities such a balancing encompasses in the information age.

B. Who Cares if You Can't Tell?

Some may be tempted to ask, "If we can't even tell whether we're at war in the information age, who really cares?" There are two responses to this. First, even though one may not know whether one is at war, the damaging effects of the attack may be very clear.[45] If someone were to use an information weapon to take down Wall Street or the Federal Reserve system, we may not know whether we are at war, but the effects of the takedown would be devastating. Second, knowing whether one is at war delimits one's responses.[46] If it could be ascertained that a foreign country had orchestrated the takedown, and that such acts constituted an illegal use of force under the U.N. Charter, one may be entitled to respond proportionately under Article 51, possibly incapacitating or deterring further attacks.[47] To the extent the attack constituted only potentially criminal acts, the response would likely be limited to investigation by the FBI and possibly other law enforcement agencies, with a view toward evidence collection and prosecution.[48]

This Article will attempt to provide a basic framework for answering the underlying question, "How do you know you are at war?," by looking first to international law, with special emphasis on the U.N. Charter, customary international law, treaties, and the U.N. General Assembly's definition of aggression.[49] This Article will then address domestic legal issues which complicate that determination. In addressing the issue, the author has specifically avoided using the term "act of war" because of the ambiguities which accompany any attempt at defining it. Instead, this Article will focus on the

---

45. *See* FIALKA, *supra* note 16, at 101–03 (outlining a scenario in which telephones fail, stock exchanges plummet, and planes are misrouted).

46. *See* U.N. CHARTER art. 51 "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs . . . . " *Id.*

47. *See id.*

48. The FBI generally has primary jurisdiction over the investigation of federal crimes. *See* 18 U.S.C. § 3052 (1994).

49. Although the issue of "state responsibility" is relevant to the discussion, due to the scope of this Article, it will not be addressed here. For an analysis of these issues outside the infowar arena, see LT. COL. RICHARD J. ERICKSON, USAF, LEGITIMATE USE OF MILITARY FORCE AGAINST STATE-SPONSORED INTERNATIONAL TERRORISM 95 (1989).

meaning of "use of force," as it may or may not apply within the IW arena, with additional consideration given to the related terms "armed attack" and "act of aggression."

III. INTERNATIONAL LAW

In attempting to define unlawful use of force, armed attack or unlawful aggression, one must first look to international law. There are potentially many sources of guidance under international law, from the U.N. Charter and other treaties, to the opinions of the International Court of Justice, to the practices of nations as exemplified in customary international law.

The collective legal guidance on the use of force is sometimes referred to as "the regime of force."[50] The importance of the regime of force cannot be understated. The resolution of its application to IW is of utmost import.

> This part of the legal order—its principles, beginning with articles 2(4) and 51 of the U.N. Charter, institutions, and procedures—is perhaps more likely than any other to be looked upon popularly as the measure of the fiber of any global culture of law and, indeed, of the real existence of an international legal system. . . . It is important practically since a breakdown of these principles threatens much greater material damage to human well-being, at least in the short run, than other areas of the international legal order. And legally the regime of force is of special importance because participants cannot legally opt out of it, unlike purely treaty-based regimes, any more than they can opt out of the legal system itself. They are stuck in both as a matter of law, just by reason of being members of the international community.[51]

---

50. *See* John Lawrence Hargrove, *Force, A Culture of Law, and American Interests*, 36 COLUM. J. TRANSNAT'L L. 433, 436–37 (1997) (noting that the regime of force, which aims to curtail large-scale violence, is the legal system "beginning with articles 2(4) and 51 of the U.N. Charter").

51. *Id.* at 436 (footnote omitted).

A. The U.N. Charter

At the time of this writing, there are 188 Member States of the U.N. Charter.[52] Some argue that even those few nations not formally Member States are nevertheless bound by the U.N. Charter because its widespread adoption has essentially transformed it into customary international law.[53]

As with many facially sweeping prohibitions, the language of Article 2(4) has not been interpreted to prohibit all use of force.[54] Its breadth is tempered both by the circumstances surrounding a use of force and other articles of the U.N. Charter.[55] A prominent commentator in the field has noted:

> Both the Charter and customary conceptions of international law with regard to use of the military instrument rested on a set of inherited assumptions about how military conflict is conducted: conflict is territorial, between organized communities; conducted by certain types of specialists in violence or "regular forces" who are clearly identified; they concentrate their efforts against each other in a war zone; the conflict itself is preceded by formal notification; suspended by some formal arrangement, and terminated in an explicit and often ceremonialized fashion.[56]

One can easily fit the First and Second World Wars into the above conception. Contrasting the above conception with

---

52. *See* U.N. Press Release, ORG/1289 *U.N. Member States* (visited Feb. 5, 2000) <http://www.un.org/overview/unmembership.html> (indicating the current number of member countries in an official press release).

53. *See* Theodor Meron, *The Meaning and Reach of the International Convention on the Elimination of All Forms of Racial Discrimination*, 79 AM. J. INT'L L. 283, 283 (1985) (observing that the U.N. Charter is accepted as the customary norm in international law). "It is generally accepted that the princples of the United Nations Charter prohibiting the use of force . . . have the character of *jus cogens*." *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 102 cmt. k (1986) [hereinafter RESTATEMENT (THIRD)] (defining *jus cogens* as peremptory norms of international law).

54. *See* U.N. CHARTER art. 2, para. 4 "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." *Id.*; *see also* Michael Reisman, *No Man's Land: International Legal Regulations of Coercive Responses to Protracted and Low Level Conflict*, 11 HOUS. J. INT'L L. 317, 319 (1989).

55. *See* U.N. CHARTER arts. 41, 42, 44.

56. Reisman, *supra* note 54, at 320.

an information war underscores the dramatic changes that have occurred since the Charter was written, and under which present legal analysis must struggle.[57] For instance, an information conflict would not generally be territorial. All points in cyberspace are essentially equidistant from each other and the damage sought in an information attack would be oriented towards damaging, destroying or manipulating data for the benefit of the attacker or to create chaos for the victim.[58] Information wars would also not generally be limited to those between organized communities.[59] A terrorist hacker or corporate spy seems more the norm to date. Information attacks are not conducted by violence specialists or "regular forces," but rather persons hacking for profit or terrorist groups who specialize in taking advantage of software "holes" or weaknesses.[60] Information wars will not be concentrated in "war zones," but perhaps more than ever will have impact on civilians through incapacitation of telephone systems, takedown of key electrical grids, or disruption of financial systems. The impact of such operations is likely to be widely felt.[61]

1. All Members

Article 2(4) does not directly address the threat or use of force by nonstate actors, such as terrorist groups and hackers acting independently of a nation-state. This can make identifying a violation of Article 2(4) difficult, as the attacked state must first determine that the source of the attack was another nation-state or agents thereof.[62] With some types of weapons this is relatively straightforward. Sophisticated satellite surveillance can capture the launch

57. *See Pentagon Lawyers See Unclear Legal Limits on Cyberwarfare* (visited Nov. 12, 1999) <http://www.infowar.com/law/99/law_110999d_j.shtml>.

58. *See generally* GENERAL ACCOUNTING OFFICE, *supra* note 23.

59. *See generally Current and Projected National Security Threats to the United States: Hearings Before the Senate Select Comm. on Intelligence*, 105th Cong. 29 (1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (listing various semi-organized threat groups).

60. *See id.* at 35–36 (examining the types of groups who might be likely to attack U.S. information systems and their methodologies).

61. *See* Munro, *supra* note 22, at 15 (analyzing possible threats to civilian infrastructures).

62. *See* Aldrich, *supra* note 12, at 100.

and flight path of nuclear ballistic missiles.[63] Unfortunately, information attacks are not nearly so easily traceable.[64] Typically, information attackers tend to take circuitous routes through the Internet to disguise their true point of origin.[65]

Article 51 provides an exception to Article 2(4) for self-defense purposes, and its self-defense provisions are not specifically limited to actions against state actors.[66] Furthermore, it is important to note that Article 2(4) and Article 51 are not coterminous.[67] Thus, not every illegal use of force in violation of Article 2(4) creates a right to self-defense under Article 51. Some illegal uses of force do not rise to the level which justifies an armed response, but rather must be dealt with diplomatically or by other means short of force.[68]

2. Threat or Use of Force

Interestingly, during the drafting of the Charter some states favored incorporating a definition of what constituted illegal aggression within the Charter.[69] The United States and other major powers opposed this position on the basis that no definition could properly account for the breadth of circumstances that necessarily would have to be accounted for in any individual case.[70] The position of the major powers

---

63. *See A Cold War Bunker Complex Readies to Fight New Enemies*, CHI. TRIB., Nov. 1, 1999, at 8.

64. *See* Aldrich, *supra* note 12, at 99.

65. For example, the 1994 Rome Labs attacks by Datastream Cowboy and Kuji started in the United Kingdom and used eight countries as jump points. *See* Duncan Campbell, *More Naked Gun than Top Gun*, GUARDIAN (London), Nov. 27, 1997, at 2.

66. *See* U.N. CHARTER art. 51. For example, the United States recently fired 80 cruise missiles at a suspected terrorist camp in Afghanistan and a suspected chemical weapons factory in the Sudan in retaliation for attacks against American embassies in Tanzania and Kenya. Intelligence linked the sites to the group suspected of responsibility for the attacks. *See* Ehsan Ahrari, *Terrorism-Proactivism: Winners and Losers*, JANE'S INTELLIGENCE REV.-POINTER, Dec. 1, 1998, at 14, *available in* 1998 WL 7898018.

67. *Compare* U.N. CHARTER art. 2 para. 4 (covering the requirement that members refrain from use of force and the threat of use of force), *with* U.N. CHARTER art. 51 (covering a member's right to respond to armed attacks).

68. *See* Oscar Schachter, *In Defense of International Rules on the Use of Force*, 53 U. CHI. L. REV. 113, 126–27 (1986).

69. *See* Doc. 810, I/1/30, 6 U.N.C.I.O. Docs. 1–2 (1945) [hereinafter U.N.C.I.O.].

70. *See id.*at 3; *see also* DEP'T OF DEFENSE, 5 DIGEST OF INTERNATIONAL LAW 740 (Marjorie M. Whiteman ed. 1965).

prevailed, thus no such definition is included in the Charter.[71]

Article 2(4) proscribes not just the actual use of force, but also the threat of the use of force.[72] The method of communicating the threat is not delimited, so communicating a threat via the Internet would be on the same theoretical footing as communicating a threat by traditional methods such as word of mouth or letter. The primary characteristic distinguishing a threat communicated over the Internet and one communicated by older methods would be in properly confirming the identity of the sender and integrity of the message based on the nature of the Internet.

Aggressive preparations for a potential conflict are not generally termed a threat of the use of force.[73] On the other hand, encouraging the organization of armed bands for incursions into another state has been deemed a violation of Article 2(4), except for those situations in which such action was requested by the host country as a part of collective self-defense.[74]

Under the concept of proportionality, a mere threat would not generally entitle one to react with force, save those special situations in which a preemptive strike could be justified as anticipatory self-defense.[75]

Whether a threat to inflict a serious information attack, such as the takedown of Wall Street, could be considered an illegal threat of a use of force would depend on several things. Some factors to consider would be the legitimacy of the threat, whether it is ambiguous, whether it is capable of being carried out, whether the threat is conditioned, and whether the threat is one of relative immediacy. Of course, whether such a threat would constitute a threat of the use of force would depend upon whether the underlying act would

---

71. *See* LELAND M. GOODRICH ET AL., CHARTER OF THE UNITED NATIONS: COMMENTARY AND DOCUMENTS 44 (3d ed. 1969); U.N.C.I.O. *supra* note 69.

72. *See* GOODRICH ET AL., *supra* note 71, at 49.

73. *See id.* (discussing preparations by France and the U.K. for possible conflict with Egypt when passage through the Suez Canal was in jeopardy).

74. *See id.* at 54; Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14 at 99–101 (June 27).

75. *See* Michael J. Glennon, *International Kidnapping: State-Sponsored Abduction: A Comment on* United States v. Alvarez-Machain, 86 AM. J. INT'L L. 746 (1992) (noting that proportionate anticipatory self-defense, is allowed if armed attack is imminent).

itself constitute a use of force, so this threshold question will first be addressed.

Does the use of force envisioned in the Charter only prohibit the use of physical force? The prevailing view among international legal scholars seems to be yes—or at least that the use of force envisioned was more in the nature of armed force versus economic or political force.[76] The latter were deemed better dealt with under the general limitation imposed by the principle of sovereign equality rather than as a Charter violation.[77] The phraseology was specifically intended to be broad, however, both to achieve a "maximum commitment" of member states, and also "more particularly to give the Security Council guidance combined with wide discretion in the interpretation and application of its responsibilities for the maintenance of international peace and security."[78]

There are, however, significant examples of non-physical uses of force that do seem to be encompassed by Article 2(4). Specifically, the provision of logistical support,[79] the use or threatened use of chemical weapons and biological weapons,[80] and aircraft radar lock-on, would all appear to violate Article 2(4).[81]

The International Court of Justice (ICJ) interpreted the scope of the use of force to include logistical support, at least under customary international law and the circumstances in the case of *Nicaragua v. United States*.[82] The case dealt with logistical support provided by the United States to the contras. There, the court held that the provision of logistical support could constitute a "threat or use of force."[83] While the court's holding would also appear to apply to Article 2(4), jurisdictional issues confined it to so holding only under

---

76. *See, e.g.*, GOODRICH ET AL., *supra* note 71, at 49.

77. *See id.* at 48.

78. *Id.* at 44.

79. *See Nicaragua,* 1986 I.C.J. at 344–46.

80. *See* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362 (1963) (discussing the use of chemical and biological weapons as violations of Article 2(4)).

81. *See* Michael N. Schmitt, *Clipped Wings: Effective and Legal No-Fly Zone Rules of Engagement*, 20 LOY. L.A. INT'L & COMP. L.J. 727, 756–57 (1998).

82. *See Nicaragua*, 1986 I.C.J. at 146–47; Reisman, *supra* note 54, at 327.

83. *See id.*

customary international law.[84] Two important classes of weapons, chemical and biological, are routinely grouped with nuclear weapons under the heading of weapons of mass destruction.[85] While both chemical and biological weapons could be delivered by a somewhat conventional looking bomb, neither requires such a delivery device.[86] A very successful attack was made on the Japanese subway system by the Aum Shinri Kyo (Supreme Truth Sect) religious group which apparently unleashed deadly sarin nerve gas by carrying it into the subways.[87] It appears quite clear that regardless of the delivery vehicle employed, the active use of these weapons by one nation against another would violate Article 2(4) as an illegal use of force.

Perhaps a closer analogy would be a radar lock-on during an aerial dog fight. At least some experts seem willing to classify such a lock-on, under certain circumstances, as unlawful use of force.[88] The same analysis would apply to radar lock-ons achieved by anti-aircraft artillery. There is a tight correlation to at least some types of IW, because the situation involves no physical force, but rather sensors which can interpret certain types of directed energy and alert the pilot through a computer display. For example, in 1998, "[a]n American F-16 launched an air-to-ground missile at [an] Iraqi missile site . . . in response to what allied forces said was evidence that radar had 'locked on' to a nearby British patrol plane."[89] When questioned about the legitimacy of such action, the Pentagon defended the pilot's action, relating that "his cockpit instruments had indicated he was

84. *See* Herbert W. Briggs, *The International Court of Justice Lives Up to Its Name*, 81 AM. J. INT'L L. 78, 83 (1987) (noting "that customary international law continues to exist and to apply, separately from international treaty law, even where the two categories of law have an identical content" (quoting *Nicaragua,* 1986 I.C.J. at 96)).

85. *See* Harvey J. McGeorge, *Bugs, Gas and Missiles*, DEF. & FOREIGN AFF., May 1990, at 14, *available in* LEXIS, News Library, Mags File.

86. *See id.* (explaining that weapons of mass destruction could be used through small droplets or fine aerosols intended for absorption via inhalation).

87. *See* Willis Witter, *Japan Seizes Subway Suspect; Followers Also Held in Gassing*, WASH. TIMES, May 16, 1995, at A1.

88. *See* Maj. Mark S. Martins, *Rules of Engagement for Land Forces: A Matter of Training, Not Lawyering*, 143 MIL. L. REV. 1, 42 (1994).

89. Michael Kilian, *Attack on Iraqi Radar Adds to Gulf Tensions*, CHI. TRIB., July 1, 1998, at 1.

being targeted, and under the rules of engagement he was allowed to respond to what he perceived to be a hostile act."[90]

On the other hand, it could be perceived as a legitimate use of a preemptive strike based on the strong presumption that when one's aircraft is "painted" by the radar of unfriendly forces, the likelihood of an imminent and deadly kinetic force attack is so great as to warrant taking preemptive action. If so justified, the analogy to IW attacks largely breaks down.

In attempting to define what is a use of force, it can be instructive to review what is not considered a use of force. Interestingly, Article 41 of the U.N. Charter appears to dismiss as uses of armed force (a slightly different, but related term) a broad swath of deleterious activities which could well be the result of an information attack. The article states:

> The Security Council may decide what measures *not involving the use of armed force* are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include *complete or partial interruption* of economic relations and of rail, sea, air, postal, *telegraphic*, *radio*, *and other means of communication*, and the severance of diplomatic relations.[91]

Thus, it appears that Article 41 sets out an additional exemption to Article 2(4)'s broad proscription against the use of force—at least when approved by the Security Council. This is so because, while it is conceivable that some of the above-enumerated measures could be accomplished without the use of armed force, very few of the measures could be accomplished without the use or threat to use physical force. What remains unclear, however, is whether economic sanctions can ever constitute a use of force.[92] The language

---

90. Martin Fletcher, *Pentagon Admits Iraqi Radar Did Not Lock-On to U.S. Plane*, TIMES (London), Nov. 4, 1996, at 12.

91. U.N. CHARTER art. 41 (emphasis added).

92. *Compare* Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 MICH. J. INT'L L. 1051, 1071–72 (1998) (stating that "a devastating economic embargo is not a 'use of force'"), *and* BROWNLIE, *supra* note 80, at 361–62 (discussing Article 2(4) and concluding that "it is very doubtful if it applies to economic measures of a coercive nature"), *with* Clinton E. Cameron, Note, *Developing a Standard for Politically Related State Economic Action*, 13 MICH. J. INT'L L. 218, 219 (1991) (contrasting the developing States'

above seems to exclude it as a use of armed force, but the language of Article 2(4) does not expressly include it as a threat or use of force.[93] This is in spite of a proposal by the Brazilian delegation to the Dumbarton Oaks Proposals to do just that. The Brazilian proposal included the term "economic measures" with the term "force," but the proposal was soundly rejected.[94] With that rejection, most Western states interpreted economic coercion to be outside the scope of Article 2(4).[95] The communist bloc and most Third World countries, however, still averred that economic coercion was within the scope of Article 2(4).[96] On the other hand, the ICJ's *Nicaragua* decision appears to hold that economic pressure does not constitute a violation of the principle of nonaggression.[97] In sum, it is unclear whether economic pressure, in and of itself, can qualify as a violation of Article 2(4).

The Charter does not further define use of force, but modifies it somewhat by speaking of the use of force in several situations: against the territorial integrity of any state, against the political independence of any state, or in any other manner inconsistent with the "Purposes of the United Nations."[98]

---

characterizations of economic diplomacy as forms of aggression with the First World States' general denial of such a view), *and* GOODRICH ET AL., *supra* note 71, at 48 (noting the disagreement among U. N. members' definition of "force" and whether economic pressure should be included).

93. *See* Lawrence T. Greenberg et al., *Information Warfare and International Law* (visited Oct. 16, 1999) <http://www.dodccrp.org/iwil> (discussing the Allied Nations view that this provision does not apply to economic coercion).

94. *See* Amendments of the Brazilian Delegation to the Dumbarton Oaks Proposals, Doc. 2, 617/e/4, 3 U.N.C.I.O. Docs. 253 (1945); Greenberg et al., *supra* note 93.

95. *See* Domingo E. Acevedo, *The U.S. Measures Against Argentina Resulting From the Malvinas Conflict*, 78 AM. J. INT'L L. 323, 327 & n.13 (1984).

96. *See id.* (citation omitted). Similarly, Third World countries attempt to define "force" as including "economic or political pressures" at the Vienna Conference on the Law of Treaties was also unsuccessful. *See* Richard D. Kearney & Robert E. Dalton, *The Treaty on Treaties*, 64 AM. J. INT'L L. 495, 533 (1970).

97. *See* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 119 (June 27). Conclusions as to the ICJ's interpretation of Article 2(4) from *Nicaragua* case must be addressed with some care. This is based on the U.S. challenge to the ICJ's jurisdiction, which prompted the Court to review the conduct under customary international law even where that body of law was arguably subsumed or supervened by Article 2(4).

98. U.N. CHARTER art. 2, para 4.

3. *Against the Territorial Integrity or Political Independence of any State*[99]

The phrase "against the territorial integrity or political independence of any state" was not originally proposed to be included in Article 2(4), but its addition was agreed to by the major powers "in response to the demand of the smaller states that there should be some assurance that force would not be used by the more powerful states at the expense of the weaker ones."[100]

a. Territorial Integrity

Use of force against the territorial integrity of another state has often been interpreted in the traditional sense as taking of land.[101] Thus, Sadaam Hussein's forcible annexation of Kuwait was clearly a violation of this provision.[102] Less clear is whether the term was meant to be equivalent to "territorial inviolability."[103] Could a country enter another country without permission, for reasons other than the taking of land, without violating the latter's territorial integrity? It appears it could not. Currently such incursions appear to be limited to those approved in treaties or other prior agreements.[104]

Less clear is how territorial integrity applies in the information age. Does one violate a state's territorial integrity by laying claim to a portion of a state's cyber real estate? Could one, for instance, appropriate a radio station or television channel by broadcasting from one's own country or some other legal position? It appears one could, at least without triggering any use of force tripwire.[105] Indeed, the

---

99. *Id.*

100. GOODRICH ET AL., *supra* note 71, at 44–45.

101. *See id.* at 47–48; U.N. CHARTER art. 2, para. 4. "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." *Id.*

102. *See* Bernard Lewis, *Who'll Win, Who'll Lose in the Gulf*, WALL ST. J., Feb. 20, 1991, at A14.

103. *See* GOODRICH ET AL., *supra* note 71, at 51–52 (asking whether "territorial integrity of a state require[s] respect for its territorial inviolability").

104. *See id.* at 51–55 (discussing the limited occasions when treaties or agreements authorize one country to use force against another country).

105. *See* International Telecommunication Convention, Oct. 25, 1973, art. 38, 28 U.S.T. 2495 [hereinafter IT Convention] ("Members retain their entire freedom with regard to military radio installations of their army, naval and air forces.") *But cf. id.*, art. 35, 28 U.S.T. at 2530 ("All stations, whatever their

Voice of America appears to be a minor manifestation of this position.[106] As discussed above, Article 41 of the U.N. Charter appears to exclude the "*complete or partial interruption of . . . telegraphic, radio, and other means of communication . . .*" from the definition of use of armed force.[107]

If interruption of the broadcast is not a use of force, what of interruption and replacement? It would appear to be far more threatening if, instead of just adding a new station or interrupting an existing station, one both interrupted the local broadcast and replaced it with one's own.[108] This would be especially true if the replacement station aimed to mimic the real station so as not to reveal its true source.[109] It is already possible for one nation to electronically hijack the signal of another nation's state-owned television station and use morphing techniques to make the replacement broadcast portray government leaders making antigovernment statements.[110]

Time magazine reported that "the Air Force's latest secret weapon" is a converted cargo plane named Commando Solo.[111] Commando Solo can purportedly "jam a country's TV and radio broadcasts and substitute messages—true or false—on any frequency."[112] Is such an IW technique an

---

purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members . . . .") *and* Convention on the Law of the Sea, Nov. 16, 1994, art. 109, 1833 U.N.T.S. 397, 438 (containing a similar provision prohibiting radio broadcasts from the high seas which interfere with the broadcasts of a State).

106. *See* Ben Barber, *Voice of America's New Leader Looks Forward to Independence*, WASH. TIMES, July 21, 1999, at A13 (reporting that some Voice of America journalists have revealed that they are ordered to cover stories based on U.S. foreign policy or public relations concerns); *see also RTS Accuses U.S. of Conducting 'Media Occupation' of Serbia*, WORLD NEWS CONNECTION, Aug. 11, 1999, *available in* 1999 WL 23693709 (reporting accusations by Radio Television Serbia (R.T.S.) that the United States is broadcasting Voice of America broadcasts over frequencies awarded by international to R.T.S. conventions).

107. U.N. CHARTER art. 41 (emphasis added).

108. *See* Greenberg et al., *supra* note 93.

109. *See id.*

110. *See* Bradley Graham, *Military Grappling with the Guidelines for Cyber War*, WASH. POST, Nov. 8, 1999, at A1 (reporting on the U.S. cyber arsenal, including the use of video morphing techniques to deceive foreign television viewers).

111. Douglas Waller, *America's Persuader in the Sky*, TIME, Aug. 21, 1995, at 43.

112. *Id.*

illegal use of force?[113] Probably not under the traditional definition, especially not under the territorial integrity stem.[114] But such an action does go beyond a strict reading of Article 41 of the U.N. Charter and could, depending on the nature of the broadcast, impinge upon the political independence of the subject state.[115]

It is less clear whether a country could pursue an information attacker electronically through the Internet, even if that pursuit required back-hacking through hubs in other countries, without violating the territorial integrity of those countries? Currently, the Department of Justice has taken the position that coordination with the affected countries is to be sought first, though it is suggested that international agreements be pursued to facilitate extending a search beyond one's borders.[116]

b. Political Independence

The threat or use of force against a state's political independence presents an issue of particular complexity. Unstable governments could in some cases be toppled

---

113. *Cf.* IT Convention, *supra* note 105, art. 37, 28 U.S.T. at 2531 (questioning whether the International Telecommunication Convention Article 37 may further constrain the information war planner when it states, "Members agree to take the steps required to prevent the transmission or circulation of false or deceptive distress, urgency, safety or identification signals . . . . ").

114. *Cf. id.* art. 38, 28 U.S.T. at 2531, 2532. It is unclear whether jamming all of a country's stations and substituting the transmissions of a belligerent, even by a quasi-exempt military radio installation, could constitute a "harmful interference." Paragraph 2 of Art. 38 states: "Nevertheless, these installations must, so far as possible, observe statutory provisions relative to giving assistance in case of distress and to the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed . . . ." The language "so far as possible" which precedes this section may afford the wiggle room necessary to circumvent this provision in time of conflict. Additionally, none of this directly addresses the issue of whether such actions constitute a use of force, rather it addresses a potential treaty violation.

115. *See* U.N. CHARTER art. 41.

116. *See Recommendation of Committee of Ministers to Member States Concerning Problems with Information Technology*, Doc. No. R(95) 13 (1995) (visited Oct. 22, 1999) <http://www.coe.fr/cm/ta/rec/1995/95r13.htm>:

> The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

through effective propaganda campaigns.[117] Indeed, the extensive power of the media suggests that a highly sophisticated and well-organized propaganda campaign may even threaten the political independence of more established governments.[118] The U.N. General Assembly adopted a non-binding Resolution on the Definition of Aggression.[119] Article 1 of the resolution largely limited the definition of aggression to the use of armed force.[120] An enumeration of what constituted armed force was set out in Article 3.[121] While this list was not to be construed as exhaustive, Article 4 made clear the term was more constrained than some third world countries had desired: "The economic, ideological and other modes of aggression were carefully considered . . . , but the result was an interpretation that they did not fall within the term 'aggression' as it has been used in the Charter . . . ."[122]

Despite the ambiguity of the terminology used in the Charter and the relatively narrow definition of aggression adopted by the General Assembly, many international law scholars still hold that, "[a]s long as the act of force . . . compels a State to take a decision it would not otherwise take, Article 2(4) has been violated."[123] Such a declaration seems somewhat circular, however, as one must still define what can constitute an act of force within the definition of a use of force.[124]

c. Or in any Other Manner Inconsistent with the Purposes of the United Nations

Article 2(4) was specifically written to try to end the tyranny of war which had so wracked the world in the First and Second World Wars.[125] This broad prohibitory phrase

---

117. *See* Greenberg et al., *supra* note 93.

118. *See id.*

119. *See* Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., Supp. No. 19, 2319th plen. mtg. at 392, U.N. Doc. A/9890 (1974).

120. *See id.* art. 1 at 393.

121. *See id.* art. 3 at 393.

122. Bengt Broms, *The Definition of Aggression*, *in* RECUEIL DES COURS, 305, 386 (1978).

123. OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 110–13 (1991).

124. *See* U.N. CHARTER art. 2, para 4.

125. *See* U.N. CHARTER preamble ("WE THE PEOPLES OF THE UNITED NATIONS DETERMINED to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, ...").

was intended to give a certain comprehensiveness and flexibility to the restriction, but necessarily not in a vacuum: "[Article 2(4)'s] interpretation and application in practice do not take place in isolation, but rather in the total context of the purposes and principles of the Charter, the responsibilities and powers of organs, and the interests and particular concerns of members."[126]

One author has suggested that the broad concluding phrase of Article 2(4)—"or in any other manner inconsistent with the Purposes of the United Nations"[127]—was meant also to serve as a catch all to include economic measures within the ambit of a threat or use of force,[128] though this construction has not been generally accepted, especially among Western countries.[129]

4. Other Articles

As was mentioned earlier, several other articles in the Charter have a role in further interpreting the scope of Article 2(4). Interestingly and somewhat confusingly, there seems to be little parallelism within the Charter between what is prohibited, when the Security Council can step in, and when any member may use force for collective or self-defense. Thus, while Article 2(4) broadly prohibits the threat or use of force, Article 39 addresses how the Security Council may react to "threat[s] to the peace," "breache[s] of the peace," or "act[s] of aggression,"[130] and Article 51 purports not to upset the inherent right of self-defense against armed attacks.[131] Somewhat inconsistent with Article 39, Article 1(1) treats "acts of aggression" as a subset of "breaches of the peace."[132]

---

126. GOODRICH ET AL., *supra* note 71, at 45.

127. U.N. CHARTER art. 2.

128. *See* Cameron, *supra* note 92, at 219 (observing that developing nations usually use economic diplomacy as a form of aggression).

129. *See id.*

130. U.N. CHARTER art. 39 ("The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.").

131. *See id.* art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.").

132. *Id.* art. 1, para 1.

And the indeterminate language of Article 1(2)[133] has actually been used to justify the use of force on behalf of independence movements,[134] though such seems to require a somewhat tortured reading of the language. Perhaps the most important article for helping to frame the issue of how we can tell we are at war is Article 51, so we will begin there.

a. Article 51 of the U.N. Charter

(i) Language

Article 51 of the U.N. Charter provides an exception to Article 2(4)'s facially sweeping prohibition against the threat or use of force:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[135]

(ii) Limitations

Of course the right of self-defense is tempered by the concepts of "military necessity" and "humanity" as defined by customary international law under the Law of Armed Conflict. The latter of these concepts encompasses the rule of proportionality.[136] This was acknowledged by the ICJ in the *Nicaragua* case: there is a "specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well

133. *See id.* art. 1, para 2.("The Purposes of the United Nations are: . . . To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace[.]").

134. *See* GOODRICH ET AL., *surpa* note 71, at 45.

135. U.N. Charter art. 51.

136. *See* Schmitt, *supra* note 92, at 1083–84.

established in customary international law."[137] The point was underscored and specifically linked to the self-defense envisioned by Article 51 in the court's decision, On the Legality of Nuclear Weapons; "This dual condition applies equally to Article 51 of the Charter, whatever the means of force employed."[138]

(iii) Applicability of Article 51 to Actions Against Terrorists

Article 51, because it has no language limiting its application to members of the United Nations, and because it purports to leave intact the inherent right of a state to defend itself, has been held to support the right to employ force against terrorists in appropriate cases.[139] Thus, one author has claimed broadly that, "A nation attacked by terrorists is permitted to use force to prevent or pre-empt future attacks, to seize terrorists or rescue its citizens when no other means is available."[140] This same author has advocated flexible legal standards in the application of force in responding to terrorist attacks. "Our military and intelligence services should be permitted under the law to prevent a terrorist attack in the same way that police officers stop a fleeing felon. As the tactics, weaponry, and targets of terrorists change, so should the legal parameters surrounding the use of force."[141] While these contentions may have visceral appeal, the weight of international legal authority seems not to go so far. "Generally speaking, a state has no right to invade a foreign state to rescue or protect its nationals who are considered to be held unlawfully by that state or by private persons."[142] There is, however,

---

137. Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 94 (June 27).

138. Legality of the Threat or Use of Nuclear Weapons (United Nations), 1996 I.C.J. 226, at para. 41 (July 8).

139. *See* GOODRICH ET AL., *supra* note 71, at 344–45.

140. Douglas Kash, *Abducting Terrorists Under PDD-39: Much Ado About Nothing New*, 13 AM. U. INT'L L. REV. 139, 139 (1997) (quoting Bureau of Pub. Affairs, U.S. Dep't of State, Current Policy No. 783, Low-Intensity Warfare: The Challenge of Ambiguity 3 (1986)).

141. *Id.* at 149.

142. Schachter, *supra* note 68, at 138–39 (citing RESTATEMENT (THIRD), *supra* note 53, § 432 cmts. b, c); *see* John F. Murphy, *Military Responses to Terrorism*, 81 AM. SOC'Y INT'L L. 287, 318–19 (1990).

> a well-established right to use limited force for the protection of one's own nationals from an imminent threat of injury or death in a situation where the state in whose territory they are located either is unwilling or unable to protect them. The right, flowing from the right of self-defense, is limited to such use of force as is necessary and appropriate to protect threatened nationals from injury.[143]

In any event, the state employing such force must be able to defend its actions through accurate and timely intelligence data supporting the choice of target(s) and the unavailability or futility of alternative means.[144]

The United States also supports broad and effective means for dealing with terrorists, unhampered by overly restrictive interpretations of international law: "We shall vigorously apply extraterritorial statutes to counter acts of terrorism and apprehend terrorists outside of the United States."[145]

b. Article 39 of U.N. Charter

Article 39 appears to provide potential support to a very expansive and flexible definition of use of force. This would be consistent with the position of many international law scholars that the U.N. Charter was designed to be a living document.[146] The article states that: "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with articles 41 and 42, to maintain or restore international peace and security."[147]

---

143. *Id.*, at 139 n.107 (quoting Statement of Ambassador Scranton, Protection of Human Rights, 1976 DIGEST § 6, at 150.)

144. Article 51 of the U.N. Charter imposes a reporting requirement on a state using force in self-defense. *See* U.N. CHARTER art. 51.

145. *Presidential Decision Directive 39*, (visited Nov. 16, 1999) <http://www.fas.org/irp/offdocs/pdd39.htm>. The language "where possible and appropriate" creates the option that the United States can act unilaterally without the consent, knowledge, or assistance of the harboring state should that state choose not to negotiate. *Id.*

146. *See* W. Michael Reisman, *The Constitutional Crisis in the United Nations*, 97 AM. J. INT'L L. 83, 83 (1993); Robert S. Winner, *SPC Michael New v. William Perry, Secretary of Defense: The Constitutionality of U.S. Forces Serving Under U.N. Command*, 3 DEPAUL DIG. INT'L L. 30, 44 (1997).

147. U.N. CHARTER art. 39.

While the terminology is different from that of Article 2(4), the language of Article 39 seems to envision a spectrum of threats, within which would fit the threat or use of force. Thus, many may choose to place threats to the peace lower on the spectrum than threats to use force. But breaches of the peace or acts of aggression would likely overlap or even be coextensive on the spectrum with the threats or uses of force. Since Article 39 allows the Security Council to "determine the existence of any threat to the peace, breach of the peace, or act of aggression"[148] without any qualification, it appears the Security Council has very broad interpretational discretion. That the Security Council could so act for the entire body is supported by Article 24: "In order to ensure prompt and effective action by the United Nations, its Members confer on the Security Council primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf."[149]

B. Customary International Law

1. Use of Force

Customary international law seems largely in accord with the above interpretation of the provisions of Articles 2(4) and 51. Indeed in the *Nicaragua* case, the United States contended that the U.N. Charter "subsumed" and "supervened" the customary international law in this area.[150] The ICJ disagreed, concluding that "customary international law continues to exist and to apply, separately from international treaty law, even where the two categories of law have an identical content."[151] The United States had asserted that under the Vandenberg multilateral treaty reservation, the ICJ lacked jurisdiction to decide any issues concerning U.S. treaty obligations.[152] In response, the ICJ agreed not to apply multilateral treaty law, relying instead on Article 36 of the Statute of the International Court of Justice[153] for its

148. *Id.*

149. *Id.* art. 24.

150. *See* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, at 92–93 (June 27).

151. *Id* at 96.

152. *See id.* at 33; *see also* Briggs, *supra* note 84, at 83.

153. *See Nicaragua,* 1986 I.C.J. at 24; *see also* Briggs, *supra* note 84, at 81–82.

jurisdiction, and customary international law for the substantive law.[154]

The court's decision was significant in that it held that the combination of logistical operations undertaken by the United States to train, arm, and equip the contras constituted both an unlawful threat or use of force and an unlawful intervention in the sovereignty of another state.[155] Laying mines without identifying their location and U.S. overflights of Nicaragua were also held to violate customary international law on non-use of force and recognition of sovereignty.[156]

2. Espionage

Some IW operations may constitute little more than the sophisticated use of technology to spy on an adversary. Spying has always been held permissible under international law and the law of armed conflict,[157] though it is almost universally outlawed under national domestic laws, and is often punished very harshly under such laws; the death penalty and life imprisonment are common maximum punishments for spying.[158] Further, the "actions of espionage or law enforcement agents within a nation's territory have never been considered a use of force under international law, ..."[159]

C. Treaties

1. On the Use of Force

Of the many treaties to which the United States is a party, those which refer to the use of force seem almost universally to use the term "threat or use of force" as a term of art without further amplification, apparently incorporating its definition under customary international law and Article 2(4) of the U.N. Charter.[160] Some treaties, like the Charter of the Organization of American States (OAS), also discuss the

---

154. *See Nicaragua*, 1986 I.C.J. at 97; *see also* Briggs, *supra* note 84, at 83.

155. *See Nicaragua*, 1986 I.C.J. at 146–47.

156. *See id.* at 147.

157. *See* Lt. Col. Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L. L. & POL'Y. 321, 330–31 (1996).

158. *See id.*

159. Kash, *supra* note 140, at 146.

160. *See, e.g.*, U.N. CHARTER art. 2, para. 4.

exceptionally broad and largely unenforced concept of non-intervention:[161]

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic, and cultural elements.[162]

The OAS treaty employs extremely expansive language, prohibiting "any other form of interference" and even "attempted threats," whatever that would constitute.[163] It is clear that this language is meant to be interpreted far more broadly than the "use of force" language of Article 2(4), but in fact the language is so broad as to be legally unenforceable.[164] Nicaragua attempted unsuccessfully to rely on this broad language in its case.[165]

---

161. For additional discussion of the law concerning non-intervention, see Lori Fisler Damrosch, *Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs*, 83 AM. J. INT'L L. 1 (1989) (discussing nonintervention in relation to nonforcible support for politics in other states).

162. CHARTER OF THE ORGANIZATION OF AMERICAN STATES art. 18 [hereinafter CHARTER OF THE OAS].

163. *Id.*

164. The complementary language in Article 19 states: "No State may use or encourage the use of coercive measures of an economic or political character in order to force the sovereign will of another State and obtain from it advantages of any kind." *Id.*, art. 19. For almost identical language, see Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, GA Res. 2131, U.N. GAOR 1st Comm., 20th Sess., 1408th plen. mtg., U.N. Doc. A/6220 (1965), and Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, GA Res. 2625, U.N. GAOR 6th Comm., 25th Sess., Supp. No. 28, U.N. Doc. A/8082 (1970). Nevertheless, it has been noted that "[a]s a legal proposition, such language is perfectly empty; for if read literally, it would outlaw diplomacy." Tom J. Farer, *Political and Economic Coercion in Contemporary International Law*, 79 AM. J. INT'L L. 405, 406 (1985); *see also* Domingo E. Acevedo, *The U.S. Measures Against Argentina Resulting From The Malvinas Conflict*, 78 AM. J. INT'L L. 323, 334 (1984) (stating economic coercion is impermissible when attempted by a state with the intent of forcing another state to adopt a particular course of action against its will).

165. *See* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27).

2. On Information Warfare

There are a myriad of treaties that could potentially impact the legality of IW attacks. These would include arrangements to which the United States is a party with countries around the world.[166] Under these agreements, each host nation's law may also come into play.[167] Additionally, the Convention on the Law of the Sea,[168] the International Telecommunications Convention of 1982,[169] and various space treaties[170] all contain limitations on actions the Member States might consider in either offensive or defensive information operations. However, while these treaties may make certain information operations illegal, they do not directly impact the issue of how one knows whether or not one is at war.

IV. LIMITATIONS

There are potentially significant limitations to employing the means necessary to detect whether one is at war under domestic and international law. As noted above, IW attacks are inherently more difficult to identify. This is because the originator's identity is easily concealed or spoofed, the attacker's association with state sponsorship is difficult to ascertain, and the attacker's intent—whether to intentionally

---

166. *See, e.g.*, Agreement Between the Parties to the North Atlantic Treaty Regarding the Status of their Forces, June 19, 1951, 4 U.S.T. 1794 [hereinafter North Atlantic Treaty Agreement]; Agreement Concerning the Status of United States Forces in Australia, May 9, 1963, U.S.-Austl., 14 U.S.T. 506 [hereinafter Australia Agreement]; Supplementary Agreement to the NATO Status of Forces Agreement with Respect to Forces Stationed in the Federal Republic of Germany, entered July. 1, 1959, U.S.-F.R.G., 14 U.S.T. 531 [hereinafter Germany Agreement]. *See also* Henry H. Perritt, Jr., *Policing International Peace and Security: International Police Forces*, 17 WIS. INT'L L.J. 281 (1999) (discussing Status of Forces Agreements' role in developing an international police force).

167. *See* North Atlantic Treaty Agreement, *supra* note 166, 4 U.S.T. at 1798, art. I.

168. U.N. Convention on the Law of the Sea, Dec. 10, 1982, U.N. Doc. A/Conf. 62/122.

169. IT Convention, *supra* note 105.

170. *See, e.g.*, Report to the United Nations General Assembly, U.N. Ad Hoc Committee on the Peaceful Uses of Outer Space, 14th Sess., U.N. Doc. A/4141 (1959); Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410; *see also* Albert N. Delzeit & Robert F. Beal, *The Vulnerability of the Pacific Rim Orbital Spectrum Under International Space Law*, 9 N.Y. INT'L L. REV. 69 (1996) (discussing the role of international space law in preventing future satellite network seizures).

or inadvertently cause harm—is oftentimes not apparent. As such, limitations on methods to detect the attacker can significantly hamper a proper determination of the severity of the situation.

A. How Does U.S. Law Apply?

According to the definitive Army Field Manual 27–100, "[a]ll military operations must comply with United States law, whether in the form of a statute, treaty or other international agreement, executive order, regulation, or other directive from a branch or agency of the federal government."[171] Certainly, it is true that by and large the military must comply with domestic law, but it seems the Field Manual overstates the case somewhat. It would seem preposterous for any military member who killed an enemy soldier during war to have to justify his actions under an affirmative defense to the crime of murder. Is it then understood that some domestic law is trumped by the law of armed conflict or the exigencies of war? Certainly the law of armed conflict, as a body of international law, would be on par with the Constitution, and therefore above other federal or state law. But the law of armed conflict, with limited exceptions, is generally concerned with setting out that which is prohibited, not in establishing affirmative substantive rights.[172]

This discord between that which is forbidden under law in peacetime America and that which may be permitted when the national security is endangered seems little explored. This is perhaps because the last war fought on American soil was over 130 years ago. The confluence between the two laws takes on increasing importance, however, in the age of IW where attacks and potential counterattacks could take place regularly within the jurisdictional boundaries of the United States. Indeed, Deputy Defense Secretary John Hamre hammered the point home when he stated, "I think everybody has to realize that we are now entering a period where we have to worry about defending the homeland again . . . I mean defending the homeland against an enemy armed with computers."[173]

---

171. U.S. DEP'T. OF THE ARMY, FIELD MANUAL 27-100 at 30–31 (1991).

172. *See* Aldrich, *supra* note 12, at 102–06.

173. *Pentagon Official Warns of Threat of Cyber-Attack*, AAP NEWSFEED, April 17, 1998, *available in* LEXIS, New Library, Non-US File.

1. Constitutional Provisions

One potential hurdle in detecting information attacks may be found in the Fourth Amendment to the U.S. Constitution.[174] It broadly protects against unreasonable searches and seizures.[175] The amendment, however, also contains a warrant clause, which allows for searches and seizures in specific circumstances. The requirement for a warrant is riddled with judicially developed exceptions, but in the area of electronic data and communications any holes seemed to have been plugged by supplementary legislation which not only fills the hole, but provides protections beyond those required by the Constitution.[176]

Case law from as recent as 1990 would suggest that whatever hurdle the Constitution provides within the United States, it will not provide much of an additional stumbling block once the trace leaves the United States. In *United States v. Verdugo-Urquidez*,[177] the Supreme Court held that Fourth Amendment protection does not extend to "the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country."[178] The Court also noted that it had previously "rejected the claim that aliens are entitled to Fifth Amendment rights outside the sovereign territory of the United States."[179] "In sum, the *Verdugo-Urquidez* opinion speaks in terms so sweeping as to suggest the general conclusion that aliens

---

174. *See* U.S. CONST. amend. IX. The Fourth Amendment sets forth certain restraints on the exercise of federal power and authority and protects people against unreasonable searches and seizures. *See, e.g.*, Weeks v. United States, 232 U.S. 383, 391–92 (1914). Evidence which is obtained by an unreasonable search and seizure is excluded from admissibility by the Fourth Amendment. *See id.* at 393.

175. *See* Maryland v. Dyson, 119 S. Ct. 2013, 2014 (1999).

176. *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030 (West 1999); Electronic Communications Privacy Act, 18 U.S.C.A. §§ 2510–2522 (West Supp. 1999); Privacy Protection Act, 42 U.S.C.A. § 2000aa (West 1994).

177. 494 U.S. 259 (1990).

178. *Id.* at 261.

179. *Id.* at 269 (citing Johson v. Eisentrager, 339 U.S. 763 (1950)). Interestingly, in *Johnson* the Court "stressed that alien litigants in that case were nationals of a country at war with the United States and had been captured while engaged in hostilities against this country." A. Mark Weisburd, *Due Process Limits on Federal Extraterritorial Legislation?*, 35 COLUM. J. TRANSNAT'L L. 379, 398 (1997). Could the same rationale apply to capturing the data or information of persons engaged in attacks against the United States? It appears the Constitution provides no bar outside the United States, provided the proper U.S. agency can track down the attackers.

residing outside the United States are not entitled to any Constitutional protections," though such a reading probably goes too far.[180] As to "alien enemies," the Court had previously held "that the Constitution does not confer a right of personal security or an immunity from military trial and punishment upon an alien enemy engaged in the hostile service of a government at war with the United States."[181] By so holding the Court narrowed the Fifth Amendment's broad language which seemingly extended its protections to any person, including enemy aliens.[182] The Court's holding, reasoned "that the Fifth Amendment offers no protection to aliens to the extent that its application would inhibit the executive's conduct of foreign relations."[183]

In *United States v. Alvarez-Machain*, the Court held that U.S. agents could enter Mexico to physically remove a person from that country and bring him to the United States.[184] Speculating about a scenario in which an U.S. agency entered via the Internet to remove or delete data, it appears the courts would find no Fourth Amendment violation, although the Computer Fraud and Abuse Act (CFAA)[185] would pose a serious stumbling block to any efforts initiated from within the United States.

2. Federal Computer Statutes

The Air Force has considered implementing "active defenses" in Air Force computer systems.[186] Active defenses would essentially operate as an electronic retaliatory strike, directing destructive programming codes at computers that actively penetrate sensitive Air Force computer systems. The Department of Justice (DOJ) has taken a position unequivocally opposed to the employment of active defenses, both because of the difficulty controlling certain types of active defenses and because it would construe such a

---

180. Weisburd, *supra* note 179, at 399 (noting that the "actual implication of *Verdugo-Urquidez* for the rights of aliens acting outside the United States . . . remains somewhat uncertain.").

181. *Johnson*, 339 U.S. at 785 (1950).

182. *See* Weisburd, *supra* note 179, at 389–91.

183. *Id.* at 394 (discussing United States v. Belmont, 301 U.S. 324 (1937)).

184. *See* 504 U.S. 655, 657 (1992).

185. 18 U.S.C.A. § 1830 (West Supp. 1999).

186. *See* Waller, *supra* note 28, at 41.

military defense to be in violation of the CFAA.[187] This broad domestic law, which brings within its ambit IW attacks, also creates a conflict as to when particular actions are dealt with as crimes and when they are dealt with as attacks against the national security.

An attempt to partially address this situation was effected with the publication of Presidential Decision Directives (PDD) 62 and 63, which established a new post of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism.[188] PDD 62 aims to provide more effective ways of combating terrorism, including "preparedness and consequent management for weapons of mass destruction."[189] PDD 63 is specifically aimed at protecting the nation's critical infrastructures.[190] It establishes a national coordinator and sets out the National Infrastructure Protection Center (NIPC) within FBI as the focus for coordinating and facilitating the federal government's response.[191] Several agencies are represented on the NIPC, including the DOD. Richard Clarke, appointed coordinator of the new post, "will chair a senior level Critical Infrastructure Co-ordination Group . . . tasked to review the vulnerabilities of government and national infrastructures and to implement information assurance policies."[192]

Of additional concern are the Electronic Communications Privacy Act of 1986 (ECPA),[193] and the Privacy Protection Act (PPA).[194] The ECPA sets out protections against the interception or disclosure of electronic communications.[195] It also "places procedural and substantive restraints on the ability of agencies to obtain warrants for criminal

---

187. *See* Interview with Susan Kelly Koeppen, Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division, U.S. Dep't of Justice (Feb. 17, 1998).

188. *See* Fact Sheet, *Combating Terrorism: Presidential Decision Directive 62*, May 22, 1998 <http://www.fas.org/irp/offdocs/pdd-62.htm> [hereinafter PDD 62]; Fact Sheet, *Protecting America's Critical Infrastructures: PDD* 63, May 22, 1998 <http://www.fas.org/irp/offdocs/pdd-63.htm> [hereinafter PDD 63].

189. PDD 62, *supra* note 188.

190. *See* PDD 63, *supra* note 188.

191. *See id.*

192. Rathmell, *supra* note 21, at 14.

193. 18 U.S.C.A. §§ 2510–2522 (West Supp. 1999).

194. 42 U.S.C.A. § 2000aa (West 1994).

195. *See* RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY, ¶ 16.11[2] (3d ed. 1997).

investigations."[196] Similarly, the PPA provides protections which extend beyond the Fourth Amendment's protections to persons involved in First Amendment activities.[197] While the aim of these laws appears to have been to provide increased protections beyond those afforded by the First and Fourth Amendments, they also provide significant hurdles to investigators or those attempting to defend against IW attacks.[198] Serious consideration should be afforded to providing national security exceptions to these laws to provide a more reasonable balance between the defense of the nation and extensions to privacy rights.[199]

3. Law Enforcement

In a far-reaching opinion, the Office of Legal Counsel advised that the FBI could legally violate customary international law and Article 2(4) of the U.N. Charter while engaging in extraterritorial abductions.[200] The opinion reasoned that the President, acting through his constitutional authority, has the power to authorize agents of the executive branch to engage in law enforcement activities in addition to those provided by statute.[201] It can be said, then, that the Office of the Legal Counsel's opinion foreshadowed the Supreme Court's position in *Verdugo-Urquidez*: "If there are to be restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty, or legislation."[202]

196. *Id.* (noting that such "statutory provisions are more restrictive than required by the constitution").

197. *See* S. REP. NO. 96-874, at 4 (1980), *reprinted in* 1996 U.S.C.C.A.N. 3950.

198. *See id.* at 3958–59.

199. *See id.* at 3971–72 (joint statement of Sens. Hatch and Simpson).

200. *See* Authority of the Federal Bureau of Investigation to Override International Law in Extraterritorial Law Enforcement Activities, 13 Op. Off. Legal Counsel 163, 164 (1989).

201. *See id.* at 176 (citing as support the Constitution's command, found in Article II, § 4, that the President "take Care that the laws be faithfully executed").

202. United States v. Verdugo-Urquidez, 494 U.S. 259, 275 (1990).

V. CONCLUSION

The U.S. military has recently been the victim of hundreds of thousands of information attacks.[203] The number of such attacks against civilian targets, which make up the nation's information infrastructure and its economic infrastructure, are more difficult to count, but are highlighted by several jarring cases. While the United States is currently the most technological and most powerful nation on earth, it is also the most vulnerable to information attacks. In light of these developments the United States must lead aggressively. It must take the lead in helping to define the contours for evaluating what constitutes the use of force in the information age.

Ultimately, what constitutes an illegal threat or use of force must focus more on the actual or potential impact of the attacker's actions than with the technological means used to achieve it. The broad language of the U.N. Charter, its construction as a living document, and the latitude it affords the Security Council in determining what amounts to a threat to the peace, a breach of the peace, or an act of aggression all provide a workable framework for applying new IW interpretations to the old terms.

While it may be desirable to address the issues in an international forum, the international community must be wary of "last wave" thinking. No longer can we afford to address the laws of armed conflict solely as they relate to the air, the land, or the sea. Nor can we limit the assessment of an aggressor's actions by its use of any particular class of weapons or even physical force. Rather, we must assess the threat to international peace by assessing the harm that occurs or is threatened. The fast-changing pace of development in the information arena will otherwise render standards useless or even detrimental within just a few months or years.

The United States must also closely review its domestic law, which currently hampers efforts to pursue and identify attackers. Lawmakers must become intimately familiar with the rapidly changing technology, which renders information attacks increasingly elusive, yet far more threatening. It will require careful balancing of the expectations of privacy

---

203. *See* U.S. GENERAL ACCOUNTING OFFICE, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, REP. NO. GAO/T-AIMD-96-92 (1996) (visited Feb. 6, 2000) <http://www.access.gpo.gov/su_docs/aces/aces160. shtml>.

against the needs of keeping our nation's infrastructure secure and defend our national security interests. Members of the DOJ, the DOD, and a key Senate Judiciary subcommittee are aware of the need for, and appear to be working toward, a means to streamline the warrant requirement for electronic pursuits, which typically crisscross a multitude of jurisdictions within the United States.

The United States must also reassess its information operations command structure. Presidential Decision Directives 62 and 63 seek to address many of the deficiencies identified by the President's Commission on Critical Infrastructure Protection,[204] but the result is still an uncertain command structure, with the FBI seemingly thrust into the position of being our nation's first line of defense to IW attacks. Still largely undefined is how and when the baton gets passed between local law enforcement agencies, the FBI, the military and the federal judiciary. Without very clearly defined roles and early involvement of the military, the United States could be hit hard and wide before the defenders even have a chance to protect critical assets or otherwise respond. Perhaps most catastrophic would be a highly structured attack disguised as a series of seemingly unrelated unstructured attacks. This would serve to weaken and distract a disjointed command structure. If followed up with a wide-reaching structured attack that hits certain critical points[205] in the infrastructure, the United States could be seriously paralyzed.

Attempts to coordinate the efforts of criminal investigators, intelligence experts, and the military are improving. Nevertheless, the current structure still places the FBI as the first line of defense in an information war.[206] But, criminal investigation can be worlds apart from national defense. One is concerned with evidence collection and preservation; the other is concerned with preservation of the

---

204. See PDD 62 and PDD 63, *supra* note 188.

205. *See* Robert David Steele, *Takedown: Targets, Tools, & Technocracy*, (visited Nov. 8, 1999) <http://www.fas.org/irp/eprint/takedown1.html> (identifying 10 especially key targets, including key bridges, levees, and dams; the Alaska pipeline, the Cincinnati rail yards; and the Culpepper communications switch, among others).

206. *See Washington Field Office Infrastructure Protection and Computer Intrusion Squad* (visited Nov. 9, 1999) <http://www.fbi.gov/program/ipcis/rccstent. html> (noting that the "FBI will also work with local and international law enforcement agencies to solve computer intrusions . . .").

national security. The importance of protecting the national security authorizes the military to use deadly force to prevent the theft of highly classified property or access to certain installations. On the other hand, civilian law enforcement agencies would generally be more concerned with properly advising the suspects of their rights and seeking appropriate search warrants in typical theft of property or trespassing cases. In a world that is becoming increasingly networked, the problems are only likely to become more complex. As such, steps must be taken now to ensure that when and if we are able to determine that we are in an information war, or any lesser manifestation which nevertheless endangers the national security, the military is not legally paralyzed in its efforts to defend that interest.