REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	14.Jan.03	THESIS

4. TITLE AND SUBTITLE
"INFORMATION WARFARE, CYBER-TERRORISM AND COMMUNITY VALIES"

5. FUNDING NUMBERS

6. AUTHOR(S)
MAJ MOORE JOE W

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

8. PERFORMING ORGANIZATION REPORT NUMBER
CI02-811

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20030225 096

14. SUBJECT TERMS

15. NUMBER OF PAGES
146

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

Information Warfare, Cyber-Terrorism and Community Values

By Joe Wesley Moore
Faculty of Law, Institute of Air & Space Law
July 2002

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the LL.M degree

Disclaimer

All views and opinions expressed in this thesis are those of the author alone and do not necessarily reflect those of any other individual, the Department of Defense, the United States Air Force, or any other government agency.

Abstract

Information Warfare involves the attack and defense of information and information systems, both in time of armed conflict and in operations short of war. While information technology provides the promise of a new class of less lethal military instruments, it also presents vulnerabilities occasioned by widespread dependence on an increasingly complex and interconnected global information infrastructure. These vulnerabilities, when exploited by those who would target civilians in order to inspire widespread fear in hopes of accomplishing a political agenda, can be understood as cyber-terrorism.

As information warfare techniques evolve, those employing them should look to several relevant sources for normative guidance. Relevant, internationally shared values can be found in international custom, the U.N. Charter, treaties dealing with the subject of "cybercrime," those governing the communication media likely to be utilized by information warriors, UNGA Resolutions and those treaties and customary norms that make up the Law of Armed Conflict.

Abstract

La guerre de l'information comporte à la fois l'attaque et la défense de l'information et des systèmes la sous-tendant, ce en temps de conflit armé et lors des opérations préalables. Bien que la technologie de l'information promette un type nouveau d'instruments militaires moins mortels, elle présente une vulnérabilité liée à la dépendance globale d'une infrastructure mondiale de l'information de plus en plus complexe et interconnectée. Cette vulnérabilité, si elle est exploitée contre des populations civiles pour répandre la peur dans l'espoir d'exécuter un programme politique, peut être entendue comme cyber-terrorisme.

Du fait de l'évolution des techniques de guerre de l'information, ceux qui les utilisent devraient considérer différentes sources normatives. Ces sources basées sur des valeurs partagées par la communauté internationale peuvent être trouvées dans le droit international coutumier, la Charte des Nations Unies, les traités relatifs à la "cybercriminalité" et aux médias de l'information potentiellement utilisables par les pirates de l'information, les résolutions de l'Assemblée générale ainsi que les traités et le droit coutumier concernant le droit de la guerre.

Acknowledgements

As always, I thank God and the U.S. Air Force for a life abundant in opportunity. While, God for always illuminated before me the path I should take, albeit not always the path I preferred, the U.S. Air Force has been His instrument in this process. I am extremely grateful for the opportunity provided, through the Air Force Institute of Technology's Civilian Institutions Program, to attend McGill University and to my former chain of command, specifically Lt Col Donald Holtz and Col Robert Kuster, for their support of my application and of my professional development in general.

To the faculty and staff of the Institute of Air and Space Law I owe my eternal thanks for a warm reception, an incredible international experience and for the benefit of their vast and varied base of knowledge. Specifically, I thank my thesis supervisor, Professor Ivan A. Vlasic, for his prodding, provocation and encouragement. His contribution, over 40 years, to the development of U.S. Air Force scholars fortunate enough to study under his direction, is surely immeasurable

To my family, the sacrifices they have made and continue to make should be recognized, not only as an enormous encouragement to me, but also as a significant service to their country. The grace and resiliency with which they endure and even treasure the vagabond lifestyle of a military family never cease to amaze me.

Finally, to my classmates, all of whom I feel privileged to call my friends, I thank them for the spirit of international cooperation and camaraderie they have provided this last year. It has been a model governments would be well served to emulate. Specific thanks are due to Liliane Pereira-Bahia from France for assistance with the French translation of the above abstract.

Table of Contents

Information Warfare, Cyber-Terrorism and Community Values

I. Introduction

This thesis will examine from an International Law perspective a burgeoning new frontier of conflict—information warfare (IW). Though a more detailed definition will follow, IW generally refers to attack on and defense of information and information systems. Thus conceived, IW can be carried out by the use of conventional weapons against elements of information infrastructure. Such an application of force has traditionally been known as command and control warfare. Increasingly, however, information and information systems have become more than just the objective; they have become the weapon, raising a new set of questions about how, if at all, the subject will be treated in international law. Though the so-called "Law of Armed Conflict" (LOAC) will likely govern many potential IW applications, IW is generally conceived of as a type of conflict that can and probably will occur in the absence of armed hostilities. Though this thesis will discuss the application of LOAC to IW, it will focus primarily on what international norms are likely to apply when LOAC does not. It will examine, *inter alia,* the Convention on Cybercrime[1], signed by 29 members of the Council of Europe and 4 other nations, including Canada and the United States in November of 2001 and discuss its possible interaction with the international law applicable to terrorism in order to formulate guidelines for determining when an act of cyber-terrorism has taken place and what

---

[1] *Convention on Cybercrime*, 23 Novemer 2001, Eur. T.S. no 185, 41 I.L.M. 282 online: Council of Europe Homepage <http://conventions.coe.int/Treaty/EN/Treaties/Word/185.doc> (date accessed: 1 July 2002) [hereinafter *Cybercrime Convention*].

an appropriate response to it would be. It will further examine the principle of non-intervention in the affairs of states, the principles relating to the threat or use of force in international relations and the legal regimes relating to the various media through which an IW attack could be carried out. The information thus developed should be of interest to military practitioners, especially those involved in the land, sea, air and space-based media through which an IW attack could occur, and others interested or concerned with the potential militarization of these media.

IW consists of an offensive and a defensive component. In the defensive context, the information warrior seeks to repel or deter attacks, which may be launched by nation-states, international terrorist organizations, transnational criminal organizations or even a juvenile hacker with a personal computer and an Internet connection. These attacks can come from any direction, are often difficult to track and cross international borders with ease. As has been aptly stated, "international borders are speed bumps on the information superhighway."[2] This feature of the threat of so-called "cybercrime" or "cyber-terrorism" can create great difficulty in combating such attacks under domestic laws. Hence, an international convention, similar to those relating to unlawful acts against international civil aviation, might be helpful in combating this menace. In fact, the aforementioned Convention on Cybercrime obligates its signatories to criminalize several acts, including illegal access to a computer system, interception of data, data interference, system interference, misuse of devices and computer-related forgery or fraud. It further requires that states cooperate in the investigation and prosecution of cybercrime.

---

[2] M. Stefik & A. Silverman, "The Bit and the Pendulum: Balancing the Interests of Stakeholders in Digital Publishing" (1999) 16 The Computer Lawyer 1.

The use of information and information systems as weapons poses two potentially conflicting policy issues. On the one hand is the need to deter and defend against information attack, while on the other is the desire to protect the right to use a non-lethal instrument in achieving national or international objectives. At a time apparently ripe to mobilize international sentiment against all forms of terrorism, it could be particularly worthwhile to canvas the relevant international treaties, agreements and resolutions in search of principles that might be helpful in formulating new norms to help states to distinguish between legal and illegal uses of IW techniques.

This thesis will first discuss in greater detail what is meant by the term, "information warfare." Though many of the technical capabilities are closely guarded secrets, sufficient information is available in the public domain to assess the types of capabilities currently being developed. A working definition will be taken from an unclassified United States Air Force Doctrine Document on the subject of Information Operations, which not only defines IW, but also breaks it down into several analytically useful components. Though the U.S. Air Force has probably the most publicly accessible operational treatment of the issue, attention will also be paid to the programs of other armed forces and other nations where available.

Attention will next turn to the threat of cybercrime or cyber-terror, looking to the nature of the threat and exploring the extent to which law might be effective in combating it. To achieve meaningful distinctions, cybercrime will be compared to IW in terms of actors, objectives and methods.

Having defined the concepts of IW and cybercrime, the thesis will canvass various international legal instruments for guiding principles that may form a useful dividing line between lawful and unlawful uses of IW. Rules of customary international law that could impact the issue will be identified. The Charter of the United Nations and those instruments and opinions underlying the internationally recognized "non-intervention principle" will also be analyzed in search of potentially applicable rules and values.

Though some scholarly attention has been paid to the application of the LOAC to IW, this thesis will take a fresh look at the issue, identifying the core concepts underlying the LOAC and discussing specific provisions of various international conventions codifying the LOAC that are of particular importance to IW. These issues will be discussed in regard to their particular application to IW in time of armed conflict and their potential to inform decisions about the use of IW techniques in operations short of war. Next, attention will turn to the legal regimes of the media comprising the global information infrastructure (GII) in search of other rules that may come into play for operations short of war. In conclusion, this thesis will seek to identify guiding principles that should be helpful in identifying cyber-criminals or cyber-terrorists and in choosing the appropriate responses to them, while also pinpointing those principles that should serve as a legal guide to the information warrior in wartime, peacetime and in between.

II. Defining Information Warfare

A. U.S. Military Definitions

An overarching definition, applicable to all of the U.S. armed forces can be found in U.S. joint military doctrine. That is the doctrine applicable to all branches of the U.S. armed forces, especially during the conduct of joint operations, those involving more than one branch. The Joint definition places IW as one subdivision of the larger concept of information operations, which are, "actions taken to affect adversary information and information systems while defending one's own information and information systems."[3] Information warfare is subsequently defined as, "IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries."[4]

1. Air Force Doctrine

The U.S. Air Force (USAF) has further refined its conception of information operations and IW in keeping with its "core competency"[5] of "Information Superiority." The further subdivision of the concept into component capabilities

---

[3] Joint Chiefs of Staff, Joint Publication 3-13, "Joint Doctrine for Information Operations" (9 October 1998) at I-1 [hereinafter JP 3-13].

[4] *Ibid.*

[5] The U.S. Air Force identifies six core competencies it sees as essential to the fulfillment of its mission. They are Air and Space Superiority, Precision Engagement, Information Superiority, Global Attack, Rapid Global Mobility and Agile Combat Support. These competencies are described in relation to basic doctrine as, "not doctrine per se, but ... the enablers of our doctrine. They begin to translate the central beliefs of doctrine into operational concepts." See U.S. Department of the Air Force, Air Force Doctrine Document 1, "Air Force Basic Doctrine" (September 1997) at 27-35.

provides a useful basis for analysis. The USAF recognizes IW as distinct from the other subdivision of information operations, "information **in** warfare."[6]

Information superiority is defined as, "the degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition."[7] Information operations, according to the USAF, are, "those actions taken to gain, exploit, defend, or attack information and information systems." Information warfare is defined as, "information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems."[8] The most significant difference between the Air Force and Joint definitions of IW is that the Air Force does not rely on the existence of a state of "crisis or conflict" to differentiate IW from IO. The Air Force instead sees both divisions of Information Operations, Information Warfare and Information in Warfare, as applying across the spectrum of conflict, from peacetime operations to full-scale war. Air Force doctrine clarifies the point; "CI [counter-information, the functional component of IW] is conducted throughout the spectrum of conflict, as appropriate and necessary, in keeping with US policy and legal requirements."[9] While this may be only a difference of semantics, the important point is that information operations (regardless of the terminology) will likely be used not only in traditional warfare but also in less intense forms of intervention.

---

[6] U.S. Department of the Air Force, Air Force Doctrine Document 2-5 "Information Operations" (5 August 1998) at 31 [hereinafter AFDD 2-5].

[7] *Ibid.* at Ch. 1, P. 2.

[8] *Ibid.*

[9] *Ibid.*

IW differs from "information in warfare" in that the former deals with information as a means of conducting operations as opposed to the role information plays as an enabler of other means of warfare. So, the use by a precision-guided missile of information derived from the Global Positioning System (GPS) does not amount to information warfare; it is instead an example of the importance of information in warfare.

2. Counterinformation

The function through which information warfare is conducted is called "Counterinformation" or CI. Counterinformation is "an aerospace function that establishes information superiority by neutralizing or influencing adversary information activities to varying degrees, depending on the situation."[10] It is further divided into Offensive Counterinformation (OCI), representing the attack component of IW and Defensive Counterinformation, representing the defense component of IW.[11]

a) Offensive

Offensive counterinformation is further divided into several roles. Those roles are psychological operations (PSYOP), electronic warfare, military deception, physical attack and information attack.[12] These subdivisions will serve as a useful conceptual framework for applying the various legal regimes to current conceptions of OCI.

---

[10] *Ibid.* at Ch. 2, P. 9.
[11] *Ibid.* at Figure 1.1.
[12] *Ibid.*

b) Defensive

The function of defensive counterinformation is likewise divided into its component roles. They are information assurance, operational security (OPSEC), counterintelligence, counter PSYOP, electronic protection and counterdeception.[13] While this thesis will deal primarily with offensive CI, the defensive component will be discussed where applicable, especially regarding developments pointing to an emerging doctrine of "active defense."

3. Army Doctrine

The Army has drafted a new doctrine document that will update its previous 1996 issuance on IO. It will define IO as "actions that target adversaries' infosystems, 'and influence others' decision-making processes, information and information systems while protecting one's own information and information systems.'"[14] The focus on influencing "others'" information systems stands in contrast to other definitions that focus on affecting "adversary" information and systems. One author has pointed to this as recognition that land forces frequently encounter "entities other than friendly forces and enemy forces on the battlefield." Specifically, the article mentions nongovernmental organizations, refugees and neutral governments.[15] To the extent Army doctrine foresees the use of information operations against these entities, this certainly raises legal issues meriting discussion.

---

[13] *Ibid.*

[14] R.H. Wright, "Information Operations: Doctrine, Tactics, Techniques And Procedures" 81:2 (1 March 2001) Military Review 30 at 31.

[15] *Ibid.*

4. Naval Doctrine

The U.S. Navy's Information Operations Strategic Plan incorporates relevant definitions from Department of Defense Instructions on the subject.[16] As such, the Navy definitions track those found in the Joint doctrine documents cited above. It is important to note, however, that the Navy envisions Information Operations occurring across the full range of the spectrum of conflict. "The Navy's IW mission is to sustain Information Superiority across the continuum of peace, crisis, and conflict enabling and enhancing the ability of naval forces to successfully execute joint military operations."[17] In further refining the Navy's conception of IW, the Strategic Plan notes, "Navy IW will be conducted as an integral part of Joint Operations; or may be executed on a standalone basis as an enabler and enhancer of service capabilities; interoperability and adherence to standards are paramount."[18] The mention of IW as a "force enabler" indicates that the Navy sees its implementation of IW enhancing its existing capabilities more so than as an independent, stand-alone strike capability. As such, the Navy appears to think of IW in much the same way that the Air Force views information in warfare.

5. Marine Corps Doctrine

Although not yet officially promulgated, a December 2001 draft doctrine document shows how the U.S. Marine Corps will likely approach IW.[19] The Marine

---

[16] U.S. Department of the Navy, "Navy Information Warfare Strategic Plan: IW—Capabilities for the New Millenium" (undated) at 4-5.

[17] *Ibid.* at 6.

[18] *Ibid.* at 11.

[19] U.S. Department of the Navy, MCWP 3-40.4, "Information Operations" (coordinating draft, 10 December 2001), online: U.S. Marine Corps Doctrine Website

Corps looks at Information Operations in terms compatible with fundamental Marine Corps doctrine. This is illustrated by the statement, "MAGTFs [Marine Air Ground Task Forces] will execute IO to enable and enhance their ability to conduct military operations consistent with our capstone concept, Expeditionary Maneuver Warfare (EMW)."[20] In other words, the Marine Corps mainly looks at Information Operations as an enabler for its more traditional mission areas. For instance, the document states, "Information Operations is an integrating concept that facilitates the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection."[21] The Marine Corps' more traditional, "information-in-warfare" approach will probably raise fewer legal questions than those of the sister services.

6. Applicability of IW Across the Spectrum of Conflict

Military operations can generally be conceived of as occurring at various points along a "spectrum of conflict." The spectrum categorizes various forms of conflict by the level of intensity of the conflict. At one extreme are peacetime and various Military Operations Other Than War (MOOTW),[22] and at the other extreme is International Warfare. As the Joint definition of the term emphasizes, "information warfare" implies an activity occurring at the latter extreme. However, the definitions employed by the various services indicate that, the word "warfare" notwithstanding,

---

<https://www.doctrine.usmc.mil/mcwp/view/mcwp3404/mcwp3404.pdf> (date accessed: 2 July 2002).

[20] *Ibid.* at 6.

[21] *Ibid.* at 5.

[22] See Joint Chiefs of Staff, Joint Publication 3-07, "Joint Doctrine for Military Operations Other Than War" (16 June 1995); Secretary of the Air Force, Air Force Doctrine Document 1, "Air Force Basic Doctrine" (1 September 1997) at Figure 1.3.

IW can, and likely will, be applied across the spectrum of conflict. Where along this spectrum a particular activity lies, could determine what legal norms apply. For instance the "Law of War" or "Law of Armed Conflict" clearly applies to conflict occurring at the upper extreme of the spectrum. Conversely, one would be hard pressed to apply the same norms to a humanitarian assistance operation. Instead, one would expect the various other sources of public international law to apply. This thesis will look at the application of information warfare across the spectrum of conflict, with special emphasis on the shifting interaction between the laws of armed conflict and other branches of public international law.

B. Background and History

One could say that IW is as old as warfare itself. Military commentators have uniformly written of the great advantage of having a superior knowledge of one's own position and that of his enemy. Sun Tzu aptly stated this maxim, "I make the enemy see my strengths as weaknesses and my weaknesses as strengths while I cause his strengths to become weaknesses and discover where he is not strong."[23] Deception has been used to tactical advantage as far back as the book of Genesis.[24] The Japanese bombing of Pearl Harbor and the allied Normandy invasion of World War II both owed their success in large measure to successful efforts at deception.

In modern conflict, however, information is taking a center stage it has never before occupied. From satellite-guided "smart bombs" to computer-networked

---

[23] Sun Tzu, The Art of War, c. 500 BC.

[24] In Chapter 34 of Genesis the sons of Jacob convinced the Shechemites that they could only marry their sisters if they were circumcised. The Schechemites complied and before their wounds were healed, Jacob's sons decimated them in retaliation for their prince's rape of their sister.

infantrymen, information has become an indispensable element of the warfighting arsenal. Though there is some debate over whether a revolution in military affairs (RMA) is underway, it can hardly be denied that information is transforming the face of conflict.[25]

Some futurists posit that information is evolving to a point where it will eventually replace physical resources as the predominate measure of power.[26] While this doesn't comport with the traditional conception of information as merely a message, it does have some validity to the new ways that information may be used in future conflict. A successful IW attack could, at least temporarily, take advantage of an adversary's superiority in terms of resources. For instance, a weapon capable of reversing the logic of the electronic systems that allow pilots to differentiate between friendly and unfriendly forces could lead pilots to confuse their own forces with those of the enemy could result in devastating and demoralizing "friendly fire" incidents, which would in turn undermine confidence in any subsequent force application missions. At the same time, it could induce pilots into enemy fire zones as easy targets.

This evolution manifests itself in contemporary practice. Command and control warfare has largely matured as a concept as evidenced by the allied effort in Operation Desert Storm. Victory was achieved with minimal casualties, to an important degree because allied forces were able to disrupt Iraq's organizational

---

[25] See generally T. Gongora & H. von Riekhoff, eds., *Toward a Revolution in Military Affairs? Defense and Security at the Dawn of the Twenty-First Century*, (Westport Conn.; London: Greenwood Press, 2000).

[26] J. Arquilla & D. Ronfeldt, "Information, Power and Grand Strategy: In Athena's Camp" in S.J. Schwartzstein, ed., *The Information Revolution and National Security, Dimensions and Directions* (Washington D.C.: Center for Strategic and International Studies, 1996) 132 at 141.

structure by targeting communication media such as the air defense network and command and control sites. The role information will play in future conflict can best be gleaned from an examination of published doctrinal statements and IW systems being developed.

C. *Known U.S. Information Warfare Capabilities*

1. Methods of Employing Offensive IW

It would be foolhardy to embark on a discussion of the legal ramifications of IW without some understanding of the ways in which it might be employed. With IW, this is somewhat complicated by the fact the IW capabilities of the U.S. and many adversaries are closely guarded state secrets, as are essential Department of Defense regulations on the subject. Nonetheless, available information does provide valuable insight into the emerging U.S. IW arsenal. The text that follows provides some examples of current IW capabilities representing the offensive IW roles discussed above.

(1) Psychological Operations (PSYOP)

The U.S. Military adopts a fairly straightforward definition to the term, "Psychological Operations," defining them more in terms of purpose than specific modalities. PSYOP are defined as:

> Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological

operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.[27]

The definition's reference to a "foreign audience" indicates that PSYOP are not aimed exclusively at opposing combatants. A significant component of PSYOP is exerting influence on the populace to undermine the national will to continue the conflict. Weapons employed in this endeavor range from relatively low-tech leaflet-carrying bombs[28] to the EC130E Commando Solo radio and television broadcast aircraft and its follow-on, the Multi-Sensor Command and Control Aircraft, reportedly on the Pentagon drawing board.[29]

(2) Electronic Warfare

"[Electronic Warfare] is any military action involving the use of [Electromagnetic] and directed-energy to control the [Electromagnetic] spectrum or to attack an enemy." [30] Electronic warfare is one of the more mature of the broader set of IW capabilities. It includes functions such as signal jamming, deceptive measures such as chaff or flares used to divert the focus of an opponents electronic detection mechanisms and the use of directed energy such as lasers, radio frequency weapons or particle beams to adversely affect an adversary's electronic capabilities.[31]

---

[27] Joint Chiefs of Staff, Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms" (12 April 2001) at 352.

[28] The Air Force Information Warfare Battlelab's website describes their leaflet bomb initiative aimed at improving the efficient delivery of "pamphlets supporting U.S. Operations." See Air Force Information Warfare Battlelab Website online: <http://afiwcweb.lackland.af.mil/battlelab/Concepts/Snapshots/index.htm> (date accessed: 21 March 2002) [hereinafter Battlelab Website].

[29] R. Wall, "USAF Defining New Special Mission Aircraft " *Aviation Week & Space Technology* 154:23 (4 June 2001) 32.

[30] U.S. Department of the Air Force, Air Force Doctrine Document 2-5.1, "Electronic Warfare" (19 November 1991) at 1.

[31] *Ibid.* at 9.

A recently unveiled component of the U.S. electronic warfare arsenal is a hand-held Global Positioning System (GPS) jammer.[32] This gives a soldier in the field the ability to deny adversaries the use of the civilian code of the GPS signal, which can normally be accessed worldwide with an inexpensive receiver that will triangulate a person's geographical coordinates.

EW operations are conducted from such air-based platforms as the U.S. Air Force's EC 130H Compass Call and the U.S. Navy's EA-6B Prowler. The conflict in Afghanistan has seen an expansion of the EA-6B beyond its traditional role as a "Suppression of Enemy Air Defenses" or SEAD aircraft to a broader range of EW functions. SEAD focuses on jamming the radar frequencies of surface-to-air weapons systems. This function is so vital that EA-6Bs are usually required to fly with strike aircraft to prevent them from being targeted. In Afghanistan, Taliban air defenses have been destroyed to the extent that this requirement has been lifted, leaving the Prowler in search of a new role. It has found this role in support of ground operations. An *Aviation Week and Space Technology* article reports, "When ... forces have been inserted behind Taliban lines or merely brought forward to support targeting on the ground, Prowlers have been suppressing Taliban communications to deny them the ability to alert forces in the rear."[33]

(3) Military Deception

---

[32] See Battlelab Website, *supra* note 28; D. A. Fulghum & R. Wall, "New Tools Emerge For InfoWar Battle" *Aviation Week & Space Technology* 154:9 (26 February 2001) 58 at 59.

[33] R. Wall, "F-14s Add Missions In Anti-Taliban Effort" *Aviation Week & Space Technology* 155:21 (19 November 2001) 38 at 39.

As stated above, deception has been a component of war throughout its history. Military philosophers have uniformly recognized its necessity in overcoming an enemy. From the Trojan Horse to the detailed deception plan that was a significant component of the allied invasion of Normandy in World War II and even to the feigning movements of the coalition forces in Operation Desert Storm, military strategy has recognized the importance of inducing one's enemy to falsely appraise his own situation and the intentions of his adversary.[34]

An aspect of deception that has received particular attention has been colloquially referred to as "perception management." Perhaps the best example of this technique is the reported use of IW techniques by U.S. Forces to insert false information into the Yugoslavian computerized air defense system in the 1998 Kosovo air campaign.[35] The potential effect of such an act was summarized in a recent issue of *Military & Aerospace Electronics*: "Take a situation where an adversary changes a database that lists the munitions available at a local facility so that the commander believes he only has enough for eight sorties, where in reality he has enough for 40. The adversary effectively has grounded 32 sorties as if he had destroyed 32 aircraft."[36]

(4) Physical Attack

---

[34] Joint Chiefs of Staff, Joint Publication 3-58, "Joint Doctrine for Military Deception" (31 May 1996) II-2.

[35] D. A. Fulghum & R. Wall, "Combat-Proven Infowar Remains Underfunded" *Aviation Week & Space Technology* 154:9 (26 February 2001) 52 at 52.

[36] J.R. Wilson,"The Terrorism Threat, Information Warfare Aims Revolve Around Countering" *Military & Aerospace Electronics* 12:10 (October 2001) 14 at 18.

Physical attack on information infrastructure represents the more traditional method of command and control warfare. However, new methods are also under development in this area. For instance, the U.S. Air Force is reportedly developing high-powered microwave weapons that could be mounted on manned or unmanned aircraft and used to scramble an adversary's computer memories and disable its electronic circuitry in key components ranging from vehicle ignitions to advance warning radar systems.[37]

(5) Information Attack

Information attack refers to, "those activities taken to manipulate or destroy an adversary's information or information system without necessarily changing visibly the physical entity within which it resides."[38] Developments in this area have for the most part remained classified. Though the classic example of an information attack would be the worms or viruses that have propagated across the Internet for years, the U.S. military is apparently focusing on capabilities with a much more predictable and focused effect.[39] The developing nature of this subset of IW is illustrated by the words of Col David Kirk, Deputy Commander of the Joint Information Operations Center, who cautioned: "You can't actually hang an operationally relevant definition on computer network warfare yet."[40] Nonetheless, the developments seem to be proceeding. Given the vastness of cyberspace, the most difficult element of

---

[37] D. A. Fulghum, "Pentagon Reveals Mobile Pain Ray" *Aviation Week & Space Technology* 154:19 (7 May 2001) 82 at 84.

[38] AFDD 2-5, *supra* note 6 at 15.

[39] D. A. Fulghum & R. Wall, "Information Warfare Isn't What You Think" *Aviaiton Week & Space Technology* 154:9 (26 February 2001)52 at 52.

[40] *Ibid.*

information attack may very well be finding an appropriate target. To aid in this, the USAF is developing advanced data analysis and modeling tools, such as "Sensor Harvest." A recent Aviation Week and Space Technology article reported, "The system essentially provides a repository of data on potential adversary countries to determine how best to launch information warfare attacks. It can be used to create 'target nomination files' that war planners can draw on."[41] The article went on to explain that it takes eight people up to seven months to create a single country file.[42] Given the time required to create a file, the data making up the database would necessarily have to be gathered in advance of actual hostilities. The degree of intrusiveness of the "harvesting" process will be an important consideration in analyzing the use of such a system.

Information Attack was attempted by the U.S. in a limited fashion in the Bosnian Conflict. According to reports, the U.S. attempted to access bank records of Slobodan Milosevic and other Serbian leaders in order to drain their funds and alter records.[43] As technology advances, one can expect that such techniques will only be used more frequently.

2. Defensive IW

Defense against IW (information assurance) is another vital aspect of DoD information policy. As the most technologically advanced force in the world, the U.S. military recognizes that it is uniquely susceptible to information attack. The

---

[41] D.A. Fulghum & R. Wall, "New Tools Emerge For InfoWar Battle," *supra* note 32 at 59.
[42] *Ibid.*
[43] E. Becker, "Computer Hackers Are Stopped; Pentagon Networks Were Victim" *The New York Times [Late Edition]* (5 March 1999) A16.

U.S. dependence on information flow is exceedingly apparent in reports of the prosecution of the "War on Terrorism" in Afghanistan. U.S. Army Brigadier General Richard V. Geraci observed, "Near-real-time video from Predator UAVs [unmanned aerial vehicles], relayed by orbiting communications satellites, is being used to identify and attack targets on the ground. And there may not be a soldier within miles of that operation. [Further,] Army space troops have been working with national agencies, putting imagery together to produce 3D 'fly-throughs.'"

To assure necessary data flow, DoD employs four defensive strategies; information environment protection, attack detection, capability restoration and attack response.[44] An interesting means of developing these capabilities is being employed by the Joint Information Operations Center at Kelly Air Force Base, TX. A specially trained team is charged with using off-the-shelf technology to develop capabilities such as signal jamming and monitoring in order to create more realistic exercise scenarios.[45] The AFIWC Battlelab is also developing defensive IW capabilities to monitor and track intrusion attempts. In the area of attack detection, the Network Attack Visualization initiative uses data visualization software to analyze large quantities of data on network events.[46] This initiative illustrates the unique vulnerabilities an IW attack could present, in that it may not be possible to detect by whom one has been attacked, or even that one has indeed been the victim of an attack.

In 1998, a report by the Global Organized Crime Project of the Center for Strategic and International Studies, Chaired by former Central Intelligence Agency

---

[44] JP 3-13, *supra* note 3 at III-1.
[45] Fulghum & Wall, "New Tools Emerge For InfoWar Battle " *supra* note 32 at 60.
[46] See, Battlelab Website, *supra* note 28.

Director, William Webster made some startling findings. The report related that in 1997 a "red team" of intelligence operatives pretending to be North Korea was able to successfully shut down large portions of the U.S. power grid and to silence the command and control systems of Pacific Air Forces in Honolulu, Hawaii.[47]

Some commentators warn of an impending "Electronic Pearl Harbor." One article observed:

> The havoc that can be wreaked online has become almost limitless. Unless you're living deep in the woods on fish you catch, chances are almost every aspect of your life is mediated through computers, from your train ride into work (thanks to computer-controlled track switches) to paying bills to relaxing in front of the television (which gets its juice from a computerized electric power grid).[48]

Many view it as only a matter of time before "rogue" states or terrorist groups attempt to exploit this opportunity. One analyst put it aptly, "If you're recruiting people to drive trucks that blow up, maybe next year you'll get someone to plant an Internet 'worm,'"[49] This prediction was apparently confirmed, according to an article in the June 27, 2002 Washington Post. The Post reports that based on computers seized from Al Qaeda camps, government experts have concluded, "terrorists are at the threshold of using the Internet as a direct instrument of bloodshed."[50] The information found on the Al Qaeda computers apparently correlated with attempts made in the late Fall of 2001 to gather information about San Francisco Bay area emergency telephone systems, electrical generation and transmission, water storage

---

[47] *Cybercrime... Cyberterrorism... Cyberwarfare...: Averting an Electronic Waterloo*, (Washington, D.C.: Center for Strategic and International Studies, 1998) [hereinafter CSIS Report] at xiii.

[48] D. Freedman, "Information Warfare" *Technology Review* 104:9 (1 November 2001) 61 at 63.

[49] *Ibid.*

[50] B. Gellman, "Cyber-Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say" *The Washington Post [Final Edition]* (27 June 27 2002) A1.

and distribution, nuclear power plants and gas facilities. The attempts were initially detected by a California police officer and traced by the FBI to telecommunication switches in Saudi Arabia, Indonesia and Pakistan.[51]

In another incident, two youths in California, at the direction of a hacker in Israel known as "the Analyzer" were able to disrupt U.S. troop movements to the Persian Gulf in February of 1998. The degree of organization and the systematic nature of the attacks led officials to initially surmise that the attacks were the work of the Iraqi government.[52]

Reports of attempted intrusions by "hackers" into Department of Defense and other government computer networks abound.[53] These anecdotal accounts are underscored by statistics compiled by DoD. According to these figures, 23,662 attempts to attack military networks were detected in 2000. That number was projected to rise to 24,000 in 2001, but had topped 34,000 by November 1 of that year.[54] The DoD further estimates that one percent of network attack attempts are successful in penetrating military networks and gaining access to unclassified military data.[55] The need to investigate and deter these attacks has led information assurance officers to seek a greater mandate to perform so-called "Active Network Defense." Active Defense would go beyond the traditional technological approaches to hacking consisting of firewalls, encryption techniques, passwords and physical security, to the

---

[51] *Ibid.*

[52] CSIS Report, *supra* note 47 at xv.

[53] See e.g. M. Janofsky, "New Security Fears As Hackers Disrupt 2 Federal Web Sites" *The New York Times [Late Edition]* (29 May 1999) A1; Becker , *supra* note 43; D. Stout, "Pentagon Acknowledges Hacker Intrusion Into a Computer System" *The New York Times [Late Edition]* (22 April 1998) A16.

[54] F. Tiboni & K. Robb, "Agencies Prepare To Hit Back At Hackers" *Federal Times* 37:42 (19 November 2001) 1.

[55] *Ibid.*

employment of new classified technology that would allow for electronic retaliation to bring an attack to a halt.[56] In blurring the line between offense and defense, this presents the vexing question of where to draw the line between military and law enforcement functions. In the U.S., this line is set by the "Posse Comitatis" Act, which generally prohibits American military members from acting as civilian law enforcement agents.

The reliance of weapon systems on information is not the only vulnerability to IW techniques. An illustration of this fact can be drawn from events surrounding the sailing of the aircraft carrier, USS Constellation, into Hong Kong harbor in August of 2001. While official information was secure and encrypted to avoid detection, the Chinese were reportedly able to monitor the approximately 20,000 private e-mail messages sent by sailors from the carrier and its escort ships.[57] Thus, the official, encrypted system was only as strong as the vigilance with which its information was safeguarded by the sailors in their private e-mails.

The vulnerabilities introduced by wireless networks are not unique to such mobile platforms as ships, however. While wireless technology has enhanced certain efficiencies in government and the corporate sector by allowing employees to access networks via laptop computers or handheld personal digital assistants (PDAs), the proliferation of radio frequency waves necessary for the operation of such a network provides a ripe opportunity for espionage. A hacking technique known as "war driving" involves driving around the perimeter of corporate or government facilities

---

[56] *Ibid.*
[57] Wilson, *supra* note 36 at 16.

with equipment designed to intercept wireless data transmission.[58] If instead of receiving signals, an adversary gets the information necessary to be able to transmit damaging messages into the network, the vulnerabilities multiply. One could imagine the same problems facing the provision of broadband Internet access via satellite. Since the data will necessarily have to travel via radio waves, the possibilities of interception and "spoofing" must be addressed.

D. U.S. Organizational Commitment to IW

The U.S. commitment to developing its IW capabilities is underscored by its substantial organizational investment in the area. While each military branch has units dedicated to incorporating IW into its arsenal, high-level Department of Defense and Joint organizations are addressing the difficult policy issues. The key adviser to the Secretary of Defense on IO matters is the Chairman of the Joint Chiefs of Staff.[59] In a significant move, responsibility for computer network attack (CNA) and defense (CND) have been consolidated under United States Space Command, headquartered in Colorado Springs, CO.[60]

The U.S. Air Force concentrates its IW efforts (other than CND and CNA) under the auspices of its Air Intelligence Agency, now under the operational control of Air Combat Command.[61] Two major subordinate organizations implement IW in

---

[58] Freedman, *supra* note 48 at 65.

[59] JP 3-13, *supra* note 3 at I-6.

[60] E. Becker, "Pentagon Sets up New Center for Waging Cyberwarfare" *The New York Times [Late Edition]* (8 October 1999) A16; D. Fulghum, "Cyber-Arsenal Needs Testing" *Aviation Week and Space Technology* 154:9 (26 February 2001) 57 at 57.

[61] D.A. Fulghum & R. Wall, "U.S. Shifts Cyberwar To Combat Commands Intelligence-Gathering, Electronic Attack and Information Manipulation are at Last Being Integrated for Combat" *Aviation Week & Space Technology* 154:9 (26 February 2001) 50.

the Air Force. They are the Eighth Air Force, headquartered at Barksdale Air Force Base in Louisiana and Air Intelligence Agency (AIA) located at Lackland Air Force Base in Texas. Under Eighth Air Force is an Information Operation Wing, consisting of five IO Groups and one Intelligence Group scattered across the globe.[62] The commander of AIA is also the commander of the Joint Command and Control Warfare Center, thus it is likely that Air Force policy about the application of IW will be reflected in the larger Joint Policy.[63]

The Air Force's IW development activities are taking place under the auspices of the Air Force Information Warfare Battlelab, a division of AIA's Air Force Information Warfare Center.[64] The Battlelab is developing both classified and unclassified IW capabilities, as mentioned above.[65]

E. Other Nations' Capabilities

Of course the U.S. is not alone in developing cyberwarfare capabilities. U.S. News & World Report quoted a senior CIA official as stating that at least a dozen countries are seriously developing significant IW capabilities. These include China, Russia, Iraq, Iran and Cuba.[66] The Center for Strategic and International Studies concluded in its 1996 report, "Eight nations have developed cyberwarfare capabilities comparable to America's. More than 100 countries are trying to develop them.

---

[62] Online: Air Intelligence Agency (AIA) Organization Chart <http://www.aia.af.mil/homepages/xp/aiaorg.pdf> (date accessed: 27 April 2002).

[63] "EW Expands Into Information Warfare" *Aviation Week & Space Technology*, 141:15 (10 October 1994) 47.

[64] AIA Organization Chart, *supra* note 62.

[65] See Battlelab Website, *supra* note 28.

[66] W.P. Strobel; "A Glimpse of Cyberwarfare" *U.S. News & World Report* 128:10 (13 March 2000) 32 at 32.

Twenty-three nations have cybertargeted U.S. systems, according to knowledgeable intelligence sources." [67]

Probably no nation is more unabashedly pursuing an IW capability than China. According to a Military Review article, "Chinese strategies rely on electrons in unanticipated ways to fulfill stratagems such as 'kill with a borrowed sword' or 'exhaust the enemy at the gate and attack him at your ease.'"[68] The Chinese general in charge of information operations recently asserted that, "new technologies are likely to find material expression in informationalized arms and equipment which will, together with information systems, sound, light, electronics, magnetism, heat and so on, turn into a carrier of strategies."[69] The Chinese, therefore, are adapting IW to more traditional Chinese military doctrine that stresses strategy as a means to overcoming technological deficiencies.[70]

The Chinese have already demonstrated their willingness and ability to engage in IW techniques on American soil. A Long Island, New York-based Webmaster associated with the Falon Gong movement, a spiritual sect that has troubled Chinese officials for years, was initially thought to be behind network attacks on the U.S. Department of Transportation. Upon further investigation, however, officials discovered that the "cyber identity" of the Falon Gong group had been stolen so that the network attack could be carried out by someone posing as a representative of the

---

[67] CSIS Report, *supra* note 47 at xvi.
[68] T. Thomas, "China's Electronic Strategies" *Military Review* 81:3 (1 May 2001) 47 at 58.
[69] *Ibid.*
[70] *Ibid.*

sect. Ultimately, the attack was traced back to the Xin An Information Service Center in Beijing, which is connected to the Chinese secret police.[71]

Other nations have engaged in varying degrees of IW as well. From low-level web page defacement to introduction of computer viruses, nations have taken to using electronic techniques in an attempt to influence political events. Defacements of Armenian websites, some of which are based in the U.S., were suspected to have originated with the Azerbaijani government. Given the history of armed conflict between Armenia and Azerbaijan, this was referred to as the first instance of a physical conflict "going online."[72] Burma's military junta is suspected of directing the "Happy 99" e-mail virus at its political opponents.[73]

III. Defining the Cyber-Terror Threat

Thus far, this thesis has focused chiefly on information warfare. A parallel and often overlapping concept is variously referred to as "cyber-terrorism" or "cyber-crime." These phrases are generally associated with criminal law, although it is not uncommon to see them used with no apparent regard for distinguishing them from Information Warfare or Information Operations. For purposes of this thesis, the phrases Information Warfare and Information Operations will be discussed within their more precisely understood meaning as military operations. Though a private individual may lack the wherewithal to conduct many of the physical attack elements of IW, most of the IW techniques mentioned in Section II above are accessible not

---

[71] Strobel, *supra* note 66.
[72] *Ibid.*, quoting Jonathan Speizer of the Open Society Institute.
[73] *Ibid.*

only to governments, but to individuals, criminal organizations and terrorist groups. The diversity of actors, along with the increasing irrelevance of national borders, will make it difficult to find the dividing line between where law enforcement action is more appropriate than military action, or whether there is in fact an area of overlap where either or both are appropriate.

Though international law generally prohibits the criminal prosecution of lawful combatants for their combat activities, terrorists are not usually considered lawful combatants, even under those circumstances where armed forces are used against them. They may not enjoy "prisoner of war" status when captured and they may not be entitled to the same due process of law considerations afforded prisoners of war under the LOAC.

The question of terrorism is important, because a nation may find it difficult to justify, on the international stage, activities which might be characterized as terrorism under its domestic laws. As these domestic laws become internationalized in the form of multi-lateral conventions, these concerns become even more patent. Especially when such evocative terms as "terrorism" dominate the discourse, one must consider whether military activities could be condemned as "state-sponsored" or "state-conducted" terrorism, jeopardizing the protections of the LOAC. Of course, a state of armed hostility has obviously been traditionally sufficient to justify that which would be murder under domestic law, leading one to question whether domestic criminal law has any relevance. However, in an age when wars are no longer formally declared, it is important to draw the line between when the more

measured limitations applied to the conduct of law enforcement activities give way to the broader freedom of action allowed in the prosecution of hostilities.

This section will examine halting efforts of the international community to outlaw terrorism. It will discuss the difficulties attendant to reaching a meaningful international consensus on the definition of the term itself. It will briefly discuss the international law applicable to the use of armed force against terrorism. It will then turn to an examination of the aforementioned Cybercrime Convention, discussing in particular when an act of cybercrime under the convention might justify a military response through the use of conventional or information warfare capabilities. It will also look to what, if any, limitations this convention and parallel domestic law may place on military uses of IW. Finally, it will examine the effect of domestic laws prohibiting military members from engaging in domestic law enforcement, including the difficulties this limitation poses in the context of cyber-attacks where the perpetrator and the perpetrator's location may not be apparent.

A. What is a Terrorist?

International efforts to deal with terrorism have met with measured success. Several treaties negotiated under the auspices of the International Civil Aviation Organization (ICAO) have been successful in mobilizing and memorializing international sentiment to criminalize certain activities generally thought of as terrorist acts.[74] These instruments, however, due to their focus on particular acts, did

---

[74] *Convention on Offences and Certain Other Acts Committed on Board Aircraft*, 14 September 1963, 20 U.S.T. 2941; *Convention for the Suppression of Unlawful Seizure of Aircraft*, 16 December 1970, 22 U.S.T. 1641; *Convention for the Suppression of Unlawful Acts Against the Safety*

not need to define the term, "terrorism." In those conventions dealing with terrorism in a broader sense, a definition of the term has been conspicuously absent, due in large measure to disagreement among states regarding so-called "national liberation movements." In other words, "One man's terrorist is another man's freedom fighter."[75]

1. United Nations Definitional Attempts

A significant milestone in the history of the United Nations' attempts to deal with terrorism was the abortive attempt, in 1972, to draft a comprehensive terrorism convention. That failure gave way to the series of conventions outlawing specific acts of terrorism mentioned above. The year 1994 marked a return to attempts to deal with the issue in general terms. In a non-binding "declaration" defining terrorism as "criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons,"[76] the U.N. focused on the underlying motive as the key indicator of terroristic conduct.

The closest thing to an internationally binding "definition" of terrorism will be found in the 2000 International Convention for the Suppression of the Financing of Terrorism,[77] should it garner sufficient ratifications to come into force. Like its predecessors, the 2000 Convention eschews an explicit definition of the term. The definition implicit in defining the offense of financing terrorism is, however, more

---

of Civil Aviation, 23 September 1971, 24 U.S.T. 565; *Convention on the Marking of Plastic Explosives for the Purpose of Detection,* 1 March 1991, 30 I.L.M. 721.

[75] A. Slaughter & W. Burke-White, "Focus: September 11, 2001--Legal Response to Terror: An International Constitutional Moment" (2002) 43 Harv. Int'l L.J. 1 at 12.

[76] *Declaration on Measures to Eliminate International Terrorism*, GA Res. 60, UN GAOR, 49th Sess., Supp. No. 49, U.N. Doc. A/49/743 (1994) at 303.

[77] *International Convention for the Suppression of the Financing of Terrorism*, 9 December 1999, 39 I.L.M. 270.

elucidating than previous pronouncements. Article 2 makes it an offense to provide financial support intending or knowing that said support will be used to carry out any of the offenses described in previous anti-terrorism treaties, or:

> Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.[78]

This broad definition has the curious effect of creating the potential of making it an internationally recognized crime to financially aid or abet actions which themselves have not been defined as criminal by the international community. Beyond this curiosity, it is important to note that in addition to classifying terrorism on the basis of its purpose, this pronouncement also looks to the status of the victim as definitive. In focusing on the intent to cause death or serious bodily injury to civilians and non-combatants, this incorporates the concept of "civilian inviolability."[79]

A recent article, appearing in the Harvard International Law Journal's evaluation of the legal implications of the 11 September 2002 terrorist attacks on the U.S., would seek to achieve the international condemnation of terrorism by incorporating civilian inviolability into Article 2 of the U.N. Charter. Slaughter and Burke-White proposed a new Article 2(4), relating to the use of force that would read, "All states and individuals shall refrain from the deliberate targeting or killing of

---

[78] *Ibid.*

[79] See generally Slaughter & Burke-White , *supra* note 75.

civilians in armed conflict of any kind, for any purpose."[80] While the authors acknowledge that at one level this approach merely shifts the definitional debate from defining "terrorism" to defining "civilian," they submit that the significant history of state practice regarding Geneva Convention law on the status of civilians will be more helpful than the intractable debates over terrorism. While this definition is broader than others in applying to the actions of states and individuals, its focus on civilians, may be unduly restrictive, given the fact that military members and installations from Khobar Towers to the Pentagon have also been subjected to terrorist attack. While it may indeed be more useful to focus on the victim than the intent of the actors, the approach taken by the Terrorist Financing Convention of protecting non-combatants would assure that military members are protected during peacetime, while recognizing that they are legitimate targets during armed conflict.

A second question raised by this approach is whether the threshold of "armed conflict" is sufficiently inclusive. The authors answer affirmatively, citing the definition of armed conflict used by the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia. That definition includes within the term "armed conflict," "protracted armed violence between governmental authorities and organized armed groups."[81] This definition, however, seems to exclude the isolated (vice protracted) incident or the actions of the terrorist acting alone (vice in concert with an armed group).

---

[80] *Ibid.* at 2.
[81] *Ibid.* at 4.

2. U.S. Definition

U.S. Domestic legislation contains at least two definitions of terrorism. Chapter 113B of Title 18, United States Code, entitled "Terrorism," generally deals with the subject in terms of the U.S. domestic criminal law, although it also creates a civil cause of action, allowing victims of terrorism to recover monetary compensation from its perpetrators.[82] Section 2331 defines international and domestic terrorism very broadly in terms of act, intent and location. In both cases, the prohibited acts are "acts dangerous to human life that are a violation of the criminal laws of the United States or of any State."[83] The *mens rea* on both occasions requires that the act "appear to be intended-- (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping."[84] While the requirement of "apparent intent" as opposed to actual intent may raise constitutional issues beyond the scope of the present thesis, the salient point for present purposes is the extent to which this definition parallels that found in the Terrorism Financing Convention.

---

[82] 18 U.S.C. §§ 2331-2339B.

[83] *Ibid.* at § 2331(1)(A), (5)(A). A slight variation exists between the two definitions in that subparagraph (1)(A) speaks of "violent acts or acts dangerous to human life," while subparagraph (5)(A) omits the reference to "violent acts," thus one could say that international terrorism, unlike its domestic counterpart consists of those violent acts that may not be dangerous to human life. Also, the domestic definition deletes the reference to acts that would be a crime if committed within the U.S., as this would be unnecessary, given the requirement that domestic terrorism actually take place within the U.S.

[84] *Ibid.* at subparagraphs (1)(B) and (5)(B). The words "by mass destruction" were added to subparagraph (a)(B) by the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001,* Pub.L. No. 107-56, 115 Stat. 272 at § 802(a)(1) [hereinafter *USA Patriot Act*]. The Act was adopted in response to the 11 September 2001 terrorist attacks. Paragraph (5), dealing with domestic terrorism, was added in its entirety by that act.

The final element of the respective definitions simply differentiates between domestic and international terrorism. Basically, a rather broad array of factors serve to provide the necessary international element to classify an alleged act as international terrorism, leaving the residual to be classified as domestic.[85]

This definition, while well suited to its apparent purpose of providing a Federal jurisdictional basis for prosecuting crimes that would otherwise be cognizable only in state courts, does not provide any differentiation on the basis of the intended victim of a terrorist act. This is not surprising given that the definition basically engrafts an additional mental state onto pre-existing crimes with pre-existing standards as to who a victim is. Also, it is not surprising that the domestic law would not address itself to the issue of combatants as victims. The statute is significant however in its re-affirmation of the *mens rea* associated with terrorism, especially when one considers that incorporation into domestic legislation, if followed by similar action by other nations, could be a manifestation of the necessary *opinio juris* for a customary rule of international law, binding on all states, to come into being.[86]

The other definition of terrorism to be found in U.S. legislation appears in Chapter 38 of Title 22, U.S. Code[87], setting forth the responsibilities of the Department of State. A definition is provided therein with reference to the responsibility of the Secretary of State to report findings regarding international terrorism to Congress.[88] That provision defines terrorism as, "premeditated, politically motivated violence perpetrated against noncombatant targets by

---

[85] *Ibid.* at subparagraphs (1)(C) and (5)(C).
[86] *Restatement (Third) of the Foreign Relations Law of the United States* § 102 (1987).
[87] 22 U.S.C. §§ 2651–2728.
[88] 22 U.S. C. § 2656f.

subnational groups or clandestine agents."[89] Once again, motivation is a key indicator of what is considered terrorism. Furthermore, this definition provides a discriminator based on the classification of the target as noncombatant. An interesting aspect of this definition is its elimination of states as perpetrators of terrorism, instead limiting those covered to "subnational groups or clandestine agents."

3. So What is a Terrorist?

Having looked at various approaches to the definition of the term, "terrorist," it may seem that there is little consensus on just what the term means. There do, however, seem to be consistent themes that run through the varying definitional attempts. Most of the definitions to be found consider political motivation in one way or another. Additionally, the concept of "civilian inviolability," finds significant support in various instruments, although usually protecting the broader group of "noncombatants." Finally, some level of violence, defined either as such or in terms such as "death" or "serious bodily injury," is required.

The question of whether a state can be a terrorist is generally not resolved, which should not be surprising given that the criminal law generally addresses itself to the acts of individuals or groups of individuals. Furthermore, the fact that a state may or may not be labeled a terrorist is really of little significance, since the principles of state responsibility discussed below will provide a sufficient basis for attributing the terrorist act of an individual or individuals to a state in appropriate

---

[89] *Ibid.* at subparagraph (d)(2).

circumstances. On the other hand, acts engaged in by a state, through its various organs, are generally more constructively dealt with by those portions of public international law dealing with intervention or the use of force.

Though Slaughter and Burke-White's "civilian inviolability" principle is intellectually attractive in that it focuses attention away from underlying motivation, which can be misused to justify reprehensible acts in the name of national liberation, it seems that the contrary view has likely gained sufficient momentum that it will predominate as this area of the law develops further. However, even though its focus on civilians as opposed to non-combatants is arguably too narrow, it is analytically worthwhile to focus primarily on the issue of unlawful targeting, since terrorist acts are equally reprehensible whether intended for political, economic or purely sociopathic reasons.

Nonetheless, two factors seem to cut across the various definitions of the term. Those are unlawful targeting and political motivation. Thus, for purposes of the present discussion, terrorism will be viewed as the targeting of non-combatants for political motives in a manner likely to cause death or serious bodily injury.

B. Military Responses to Terrorism

While terrorism is largely understood as a criminal offense and widely treated as such, that is not to say that law enforcement provides the only mechanism of response to terrorism. If international consensus on the permissibility of a military response to terrorism did not exist prior to September 11, 2001, it would be difficult

to deny that it has emerged since that time.[90] While that extreme case is useful in establishing the proposition, a closer examination will be required to assess the particulars of under what circumstances military action is preferable to, or complementary of law enforcement action. As one author noted in 2000, "States do not today challenge the view that actions by irregulars can constitute armed attack; the controversy centres on the degree of state involvement that is necessary to make the actions attributable to the state and to justify action in self-defence in particular cases."[91] Finding this dividing line is particularly necessary in the context of cyber-terrorism, given that the effects of a cyber-attack may not be as drastic but could be even more pervasive in terms of individuals directly impacted.

1. State Responsibility for Terrorism

Since armed conflict is widely understood as an activity that takes place between sovereign states, and the use of force within the territory of a state without justification is generally seen as a breach of that state's sovereignty, the threshold question one must answer when contemplating the use of military force abroad in response to criminal activity regards state responsibility. This facet of international law attempts to define those circumstances under which a state can be held internationally responsible for the actions of its nationals or those operating within its borders or with its assistance.

---

[90] For a good summary of the international acquiescence in, if not support of, the U.S.-led response to these incidents, see S. Murphy, "Terrorism And The Concept Of 'Armed Attack' In Article 51 Of The U.N. Charter" (2002) 43 Harv. Int'l L.J. 41 at 48.

[91] C. Gray, *International Law and the Use of Force*, (New York: Oxford University Press, 2000) at 97.

a) The International Law Commission Draft Rules

A useful beginning point for this analysis is the attempt by the International Law Commission to codify the rules of state responsibility. The draft articles on responsibility of States for internationally wrongful acts are annexed to U.N. General Assembly Resolution 56/83, which takes note of the articles and commends them to the consideration of states.[92]

Under the ILC draft rules, state responsibility attaches to acts fulfilling two requirements. The act in question, which may be "an action or omission," must be attributable to the state under international law and it must amount to a breach of an international obligation.[93] The pertinent question for present purposes regards the issue of when an act is attributable to a state. The ILC draft rules provide a rather conservative list of factors justifying state attribution. The list begins with the more obvious criteria such as that the conduct was that of an organ of the state or of an individual exercising state authority, even when acting in excess of actual authority.[94] Likewise, conduct directed or controlled by the state will lead to state attribution.[95] Regarding insurrectional movements, the ILC draft rules only make their actions attributable to the state if they are successful in becoming the new government of the state or establishing a new state.[96] Regarding individuals not exercising government

---

[92] *Responsibility of States for Internationally Wrongful Acts,* GA Res. 56/83 UN GAOR, 53rd Sess., UN Doc. A/56/PV.85 (2002) [hereinafter ILC draft Rules]. Regarding the weight to be given ILC pronouncements, see *infra* section IV.A.3.

[93] *Ibid.* at Article 2.

[94] *Ibid.* at Articles 4-7.

[95] *Ibid.* at Article 8.

[96] *Ibid.* at Article 9.

authority or representing government organs, their acts are only attributable to states if they are acknowledged and adopted by the State as its own.[97]

These rules, if viewed as exhaustive, would allow states to provide significant support to terrorists and terrorist organizations, while evading state responsibility by simply refraining from directing and controlling the actions of the terrorists and failing to acknowledge and adopt their actions once committed. As one author noted, "The traditional 'effective control' test for attributing an act to a state seems insufficient to address the threats posed by global criminals and the states that harbor them."[98] Professor Reisman provides another eloquent criticism; "Because ... the prescriptive regime that the international decision process has created tends to shield the state principals who order or finance terrorism, this part of international law, the intentions animating it notwithstanding, may actually encourage rather than deter terrorist adventures."[99]

The list provided by the ILC draft rules should not, however, be viewed as an exhaustive pronouncement. This is made clear by Article 55 of the rules themselves, which clarifies that they do not apply to the derogation of special rules of international law providing for state responsibility. The 1970 Resolution on Friendly Relations could be seen as providing such special rules requiring states to "refrain

---

[97] *Ibid.* at Article 10.

[98] Slaughter & Burke-White, *supra* note 75 at 20.

[99] W.M. Reisman, "Symposium: Legal Responses to International Terrorism" (1999) 22 Hous. J. Int'l L. 3 at 60.

from organizing, instigating, assisting, or participating in ... terrorist acts in another state or acquiescing in ... activities ... directed towards the commission of such acts"[100]

Furthermore, it would not take an extreme feat of creativity to attribute terrorist activities to an "action or omission" of a governmental authority. As another author noted with regard to the responsibility of the Taliban regime for the 11 September attacks:

> Depending on the facts, one might find the de facto government responsible because of the omissions of its organs or officials in allowing Al Qaeda to operate from Afghanistan even after its known involvement in terrorist acts prior to the September 11 incidents (Articles 2, 4-5), because the de facto government by default essentially allowed Al Qaeda to exercise governmental functions in projecting force abroad (Article 9), or because after the September 11 incidents the de facto government declined to extradite Al Qaeda operatives and thus, in effect, adopted Al Qaeda's conduct as its own (Article 11).[101]

In fact this author contends that the right of military response to terrorism transcends the issue of state responsibility. He observes that while Article 2 of the U.N. Charter prohibits the use of force by one state against another, Article 51, recognizing the inherent right of self-defense, does not limit that right to defense against the actions of states.[102] This view notwithstanding, the majority of authors require some basis for attributing terrorist acts to a state as a prerequisite to an armed response.[103] Indeed,

---

[100] See, Slaughter & Burke-White , *supra* note 75 at 11, quoting *Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism*, G.A. Res. 210, U.N. GAOR, 51st Sess., Supp. No. 49, at 346, U.N. Doc. A/51/631 (1996); and R. Erickson, *Legitimate Use of Military Force Against State-Sponsored International Terrorism*, (Maxwell AFB AL: Air University Press, 1989) at 121, citing *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States*, G.A. Res. 2526(XXV), U.N. GAOR, 25th Sess., Supp. No. 28, UN Doc. A/8028 (1970) [hereinafter *Declaration on Friendly Relations]*.

[101] Murphy , *supra* note 90 at 50-51.

[102] *Ibid.*

[103] See, I. Brownlie, *International Law and the Use of Force By States*, (London: Oxford University Press, 1963) at 369-372, Y. Dinstein, *War, Aggression and Self-Defense*, 3rd ed.

this approach gives appropriate weight to state sovereignty, while the rules of state responsibility are capable of being interpreted broadly enough to serve legitimate self-defense concerns.[104]

b) The ICJ and Customary International Law

The application of the Resolution on Friendly Relations requires an examination of the opinion of the International Court of Justice (ICJ) in the *Nicaragua* case.[105] The ICJ relied heavily upon the Resolution in finding the necessary *opinio juris* to support its findings that the customary international law prohibits (in the absence of an exception to the principle) the threat or use of force in international relations and further prohibits (again absent a recognized exception) intervention in the internal affairs of sovereign states.[106] Given the treatment of this resolution in the *Nicaragua* case, its unanimous adoption by the U.N. General Assembly and the frequency with which it has been cited in the literature for the more than 30 years since its adoption, at least certain of the principles articulated therein could be said to represent customary international law.

The *Nicaragua* case raises serious questions relevant to the present inquiry that must be answered by one seeking to justify the use force in response to acts of terrorism. State responsibility was an issue in that case regarding the degree to which

---

(Cambridge: Cambridge University Press, 2001) at 181-3; Reisman, *supra* note 99 at 48-49; Gray, *supra* note 91 at 126.

[104] A more controversial aspect of the military response to terrorism relates to the response to terrorism perpetrated against nationals abroad. A clear international division of opinion surrounds this question, which will not be discussed in depth in this thesis, given the unlikelihood of a cyber-attack against nationals abroad being used as a justification for an armed response. For a good discussion of the debate, see Gray, *supra* note 91 at 108-110.

[105] *Case Concerning Military And Paramilitary Activities In And Against Nicaragua (Nicaragua v. United States of America)(Merits)*, [1986] I.C.J. Rep. 14 at 100.

[106] *Ibid.* at 106.

the Court viewed the U.S. as responsible for alleged violations of humanitarian law by the Nicaraguan *contras* in the course of their campaign against Nicaragua's governing junta. While the Court found the U.S. engaged in an unlawful use of force and an unlawful intervention by virtue of providing funds, training, arms and intelligence to the *contras*, it did not find that these activities constituted the necessary "effective control" to render the U.S. responsible for alleged atrocities of the *contras*. The U.S. was instead held responsible, independently of the acts of the *contras*, for its use of force and intervention as found by the Court.[107] The Court apparently viewed the Resolution on Friendly Relations as a source of distinct obligations, the violation of which could be characterized as a wrongful intervention or even a use of force, but, at least in the context of that case, not as an "armed attack" justifying an armed response. Importantly, the Court did not use the Resolution as a basis for imputing state responsibility.

A further significant holding from the *Nicaragua* case involves the Court's finding that support provided by Nicaragua to rebels in El Salvador did not justify a forceful response by the U.S. in collective self-defense of El Salvador. The primary basis of this holding, however, is the lack of a contemporaneous credible request for assistance from El Salvador, leaving largely open the question of whether El Salvador would have been justified in an armed response.[108] Significantly, however, the court held that an "armed attack" does not include, "assistance to rebels in the form of the provision of weapons or logistical or other support."[109]

---

[107] *Ibid.* at 65.
[108] *Ibid.* at 127.
[109] *Ibid.* at 104.

c) State Practice Since *Nicaragua v. U.S.*

While the *Nicaragua* case would seem to largely foreclose an armed response to terrorist acts absent a finding of "effective control," the ICJ did not purport to be describing immutable principles. Quite to the contrary, they noted, "Reliance by a State on a novel right or an unprecedented exception to the principle [of non-intervention] might, if shared in principle by other States, tend towards a modification of customary international law."[110] This undoubtedly states a principle applicable beyond the mere question of intervention. As such, it calls for an examination of state practice since 1984.

Historically, Israel and the U.S. have been the chief proponents of the use of force in response to terrorism. Israel took such action in 1968 in Lebanon and in 1985 against Tunis. The U.S. did so against Libya in 1986, Iraq in 1993, and Sudan and Afghanistan in 1998. Their forceful responses, at least prior to the 1993 attack on Iraq have generally met with widespread condemnation by other states.[111] Some commentators point to the 1993 cruise missile attacks against Baghdad in response to an uncovered Iraqi assassination plot against former president, George Bush, as a turning point.[112] China stood alone in condemning the U.S. for this use of force, while other nations expressed varying degrees of understanding, if not support, for the American position that the action was an exercise of self-defense.

Since that time, the U.S. has initiated missile strikes against Sudan and Afghanistan in response to terrorist bombings of U.S. embassies in Kenya and

---

[110] *Ibid.* at 109.
[111] Gray, *supra* note 91 at 115-6.
[112] *Ibid.* at 117; S. Baker, "Comparing the 1993 U.S. Airstrike on Iraq to the 1986 Bombing of Libya: The New Interpretation of Article 51" (1994) 24 Ga. J. Int'l & Comp. L. 99.

Tanzania. While the attack on Sudan drew localized criticism from the League of Arab States, Russia and seven other Middle Eastern nations, the strikes on Afghanistan failed to attract significant condemnation and received varying levels of support from Australia, France, Germany, Japan, Spain, and the United Kingdom.[113] The widespread support of the U.S. action against the Taliban after September 11, 2001, would appear to confirm that state practice has moderated the rather stark "effective control" test enunciated in the *Nicaragua* case, such that a terrorist attack will more likely be considered an armed attack imputable to a state and justifying the use of force in self-defense. The limitations found in the principles on friendly relations would seem to be a preferable means for assessing state responsibility. The words "organizing," "instigating," "assisting," "participating" and "acquiescing" all contain some element of knowledge, assuring that states will not be held responsible without some level of knowing involvement. At the same time, these terms recognize the reality that states can and do participate in terrorist acts in ways that, while falling short of "effective control" are nonetheless equally reprehensible.

2. Requirements Beyond Attribution

The attribution of a criminal act to a particular state, in and of itself, is not sufficient to justify a military response. In fact, the use of military force to settle interstate disputes is generally prohibited.[114] The ILC draft rules arguably attempt to limit a state's responses further by mandating substantive and procedural prerequisites to the exercise of countermeasures in response to a wrongful act

---

[113] Riesman, *supra* note 99 at 49.
[114] U.N. Charter, Article 2.

attributed to a state.[115] The U.S. State Department takes issue with these provisions, stating that they go beyond codifying customary international law and commenting specifically, "We are concerned that such a blanket constraint on the use of countermeasures provision could be exploited by the responsible State to the further detriment of the injured State."[116] The U.S. suggestion to modify, or in the alternative, delete the provisions relating to countermeasures was not followed in the draft eventually submitted, which could pose a significant barrier to widespread acceptance of the principles. In the meantime, the better approach is probably to consider an act attributable to a state within the existing framework relating to the legal resort to use of force under the U.N. Charter and/or customary international law relating to countermeasures. These issues will be discussed more fully in Chapter IV of this thesis.

C. *The Distinction Between Terrorism and Combat*

As the previous discussion attests, an important element of most definitions of terrorism involves the targeting of non-combatants. This is important not only because of the protection afforded civilians, but also in drawing the distinction between terrorism and combat. While many combat operations involve the same methods as terrorism, the LOAC, which will be discussed more fully in Section IV (E) *infra,* contains a comprehensive and well-defined regime for the protection of

---

[115] For instance, an aggrieved state must first notify the offending state and request that they fulfill their obligations, must notify of any contemplated countermeasures and offer to negotiate, and cannot respond if the violation has ended. See ILC Draft Rules , *supra* note 92 at Article 52.

[116] U.S. Department of State, "United States Statement, 55 UNGA Sixth Committee, Agenda Item 159, Report of the International Law Commission" October 27, 2000, online: State Department Web Page < http://www.state.gov/documents/organization/6598.doc>.

civilians in armed conflict. Thus, an important aspect of the law regarding responses to terrorism is the protection afforded civilians in contexts not covered by the LOAC. If one accepts as axiomatic that different rules pertain in times of war than in times of peace, one must also accept that a fundamental question is the dividing line between these two states of affairs.

Two requirements are generally required for a particular action to fall within the coverage of the LOAC. First, the activity must take place during a state of armed conflict, and second, it must be conducted by a lawful combatant. That an action fails to meet either of these criteria should result in that action being evaluated under the peacetime law. It should be recognized that the intersection of this concept with that of state responsibility provides a corresponding overlap in terms of permissible responses. For example, the act of a civilian, either in time of war or peace, would be evaluated in terms of the criminal law to the extent the civilian is not a lawful combatant. If the act were also attributable to a state, the existence or non-existence of a state of armed conflict would determine whether the conduct would be evaluated in terms of the *jus ad bellum*, governing the permissibility of resort to force, or the *jus in bello*, governing the manner in which force may be applied.[117]

1. When Does Combat Begin?

Traditionally, the existence of a state of war depended upon such formalities as a declaration of war. This principle was enshrined in the Convention (III) Relative to the Opening of Hostilities of 1907, which required either a declaration of war or an

---

[117] Erickson, *supra* note 100 at 57-94.

ultimatum with a conditional declaration of war.[118] In the U.N. era; however, a formal declaration of war has been the rare exception. There is nonetheless widespread agreement that the application of the LOAC, a subset of "International Humanitarian Law," no longer depends upon a formal declaration of war for it to apply.[119] Instead, the operative state of affairs has become the existence of an "international armed conflict."[120]

This concept is confirmed in the common Article 2, paragraph 2 of the Geneva Conventions of 1949, which provides that the conventions apply, "to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[121] Though the term, "armed conflict" is not defined in the Geneva Conventions, the International Committee of the Red Cross, in its commentary to the Conventions defines the term quite broadly as, "Any difference arising between States and leading to the intervention of members of the armed forces...."[122] Though state practice has not treated all military clashes as armed conflict, raising the question of whether the clash must reach some minimal level of intensity or duration,

---

[118] *Convention (III) Relative to the Opening of Hostilities*, 18 October 1907, 36 U.S. Stat. 2259, also available in D. Schindler & J. Toman, eds., *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions and Other Documents* (Dordrecht, Netherlands: Marinus Hijhoff Publishers, 1988) at 57.

[119] C. Greenwood, "Scope of Application of Humanitarian Law" in D. Fleck, ed., *The Handbook of Humanitarian Law in Armed Conflicts* (Oxford: Oxford University Press, 1999) 39 at 39-40.

[120] *Ibid.*

[121] *Ibid.* at 57, citing *Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 12 August 1949; 75 U.N.T.S. 31; *Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, 12 August 1949, 75 U.N.T.S. 85; *Convention (III) Relative to the Treatment of Prisoners of War*, 12 August 1949; 75 U.N.T.S. 135; *Convention (IV) Relative to the Protection of Civilian Persons in Time of War*, 12 August 1949, 75 U.N.T.S. 287 [Hereinafter: Geneva (I), (II), (III) and (IV), respectively], also available in Schindler & Toman, *supra* note 118 at 373, 401, 423 and 495.

[122] Greenwood, *supra* note 119 at 42.

in general terms it is "the use of force by the organs of a state" that is generally understood as the threshold for the application of the LOAC.[123] In the context of a response to a terrorist act, the terrorist act would not be protected by the LOAC because it was not committed by an organ of the state, yet it could be attributable to the state such as to justify a forceful response that would fall within the ambit of the LOAC.

It is also fundamental that the LOAC applies without reference to whether the particular use of force bringing it into being is lawful.[124] This only makes sense, since both sides in an armed conflict invariably seek to portray the other as the aggressor. If being so labeled excused one's opponents from their obligations under the Humanitarian Law, its application would become entirely illusory.

2. Who are Lawful Combatants?

Even in time of armed conflict, only the actions of lawful combatants are governed by the LOAC. In this context a person is either a non-combatant (civilian), a combatant or an unlawful combatant. Non-combatants are generally considered illegal targets. The status of combatant entitles a person to prisoner of war status and to lawfully participate in hostilities free from the sanction of the peacetime criminal law. Thus, the killing by a soldier of a soldier or a civilian during a time of armed conflict would be evaluated in terms of whether it comported with the tenets of LOAC, not under the criminal statutes relating to homicide. Finally, the term "unlawful combatant" generally applies to civilians who take part in conflict or those

---

[123] *Ibid.*, See also, I. Detter, *The Law of War*, 2nd ed. (Cambridge: Cambridge University Press, 2000) at 135-148.

[124] Greenwood, *supra* note 119 at 45.

combatants who forfeit their protections under the LOAC by virtue of failing to comply with certain provisions of the LOAC. Unlawful combatants are "often summarily tried and enjoy no protection under international law."[125]

The 1949 Geneva Conventions delineate the characteristics that identify combatants. They are those:

> (a) commanded by a person responsible for his subordinates;
>
> (b) Having a fixed distinctive sign recognisable at a distance;
>
> (c) carrying arms openly;
>
> (d) conducting their operations in accordance with the laws and customs of war.[126]

A chief purpose of these requirements is clarified by the 1970 Additional Protocol I to the Geneva Conventions, requiring that combatants "shall be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict."[127] One is not entitled to the benefits of combatant status unless he is subject to an effective disciplinary mechanism to enforce the responsibilities imposed by the LOAC and is readily identifiable as a combatant.[128]

---

[125] Detter, *supra* note 123 at 148.

[126] Geneva (I), *supra* note 121 at Article 13.

[127] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977 16 I.L.M. 1391, available in Schindler & Toman, *supra* note 118 at 621 [hereinafter *Additional Protocol I*] at Article 43.

[128] A discussion of the conditions under which irregular, militia or police forces might be considered combatants is beyond the scope of the current discussion. The topic is well-addressed in Detter, *supra* note 123 at 135-150.

D. Cyber-terrorism and the Cybercrime Convention

On November 11, 2001, 26 nations of the Council of Europe and four other nations signed the Cybercrime Convention in Budapest. Since that time, three other European states have signed the instrument.[129] The Convention represents a significant development toward achieving the necessary international cooperation to effectively combat criminal activity that, by its nature, is often too elusive to be contained within the constraints of domestic law. It defines several offenses and provides mechanisms for international cooperation in investigation and prosecution of offenses and/or the extradition of offenders.

1. Relevance of Criminal Law

While the Convention does not exempt the activities of states from its coverage, its clear intent is to govern the conduct of individuals, groups of individuals and legal persons such as corporations. Nonetheless, the Convention's international recognition of such values as data integrity and individual privacy may serve as a basis, when applied in conjunction with the principles of state responsibility, for a conclusion that their violation by states represents an actionable wrong, especially in the absence of a state of armed hostility. To the extent a violation is the subject of state responsibility, the full range of countermeasures under international law, to include the threat or use of force, would have to be evaluated. A crime defined under the Convention might, if perpetrated for political purposes against non-combatant

---

[129] Table of Signatories and Ratifications, online: Council of Europe Webpage <http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=&DF=> (date accessed: 11 May 2002).

targets in a manner likely to cause death or serious bodily injury, be considered "cyber-terrorism." Such a narrow definition should prove more analytically useful than the journalistic hyperbole with which the term is often used. When viewed in light of the Principles of Friendly Relations, responsibility could attach to those states seen as assisting or acquiescing in acts of cyber-terrorism.

2. Prohibited Activities

Of the five broad categories of offenses the signatories of the Cybercrime Convention undertake to criminalize, two are of particular relevance in the context of information warfare and/or cyber-terrorism. Those are "offenses against the confidentiality, integrity and availability of computer data and systems" and "computer-related offences."[130]

a) Offenses Against Data and Systems

The Convention defines five offenses against data and data systems. They are illegal access, illegal interception, data interference, system interference and misuse of devices. Each will be discussed further below.

(1) Illegal Access

Article 2 deals with intentionally accessing "the whole or any part of a computer system without right."[131] The signatories, by this provision, seek to outlaw

---

[130] *Cybercrime Convention*, *supra* note 1at Title1, Title 2. Title 3, related to content-related offences such as child pornography, Title 4 related to copyright infringements and Title 5 related to ancillary liability (i.e. attempts, aiding and abetting), while furthering significant community values, will not be discussed herein, as they are more generally associated with individual criminal behavior unlikely to be attributed to states.

[131] *Cybercrime Convention*, *supra* note 1 at Article 2.

the activity commonly termed, "hacking" whereby individuals attempt to circumvent security measures designed to prevent their access to computer systems. While merely gaining access to information systems, without more, is unlikely to cause physical or personal destruction, this provision recognizes the value of system integrity as a protectable interest.

(2) Illegal Interception

Illegal interception includes, "interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data."[132] This differs from the previous provision in that it is access to data as it moves within or between systems that is forbidden. The provision also clearly prohibits the practice of "war driving" mentioned above, whereby electronic sensors are used to gather electromagnetic information from the environment.

(3) Data Interference

Article 4 prohibits the intentional, "damaging, deletion, deterioration, alteration or suppression of computer data without right."[133] This offense deals with acts that go beyond merely looking at data to the more malicious acts of actually changing information. Depending on the target, this level of activity could range from the nuisance of web-page defacement to wide-ranging loss of life that could be caused by manipulating railroad switches, air navigation information, pipeline

---

[132] *Ibid.* at Article 3.
[133] *Ibid.* at Article 4.

management software or the like. Thus, an act in violation of this provision could, under appropriate circumstances, be considered cyber-terrorism and given the right facts be attributable to a state, bringing the analysis of whether a response by force would be required into the picture.

(4) System Interference

Article 5 expands on the previous article by proscribing, "when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."[134] In addition to expanding the concept of data interference to the system level, this provision deals with the "denial of service attack" whereby the perpetrators flood a system with otherwise legitimate traffic for the purpose of overloading the system, diminishing or even eliminating the functionality of the system.

In the context of government action, it should be noted that access and interception are activities that might be expected in the intelligence and law enforcement communities. Data and system interference, on the other hand, are exactly the types of capabilities being developed and employed in the conduct of information warfare, raising the issue of when it is appropriate for states, through their organs, to act in ways increasingly recognized on the international scene as illegal when conducted by individuals. The closest thing to a clear line is that between armed conflict and peacetime, mentioned above. For that reason, these

---

[134] *Ibid.* at Article 5.

provisions should be given great weight by those contemplating the use of IW techniques outside of the context of an "armed attack."

(5) Misuse of Devices

The final offense against systems and data is entitled, "Misuse of Devices." It deals with the manufacture, sale and use of devices or computer programs or the dissemination of passwords for the purpose of committing any of the offenses listed above.[135] While it might be tempting to conclude that military laboratories should consider these limitations when developing information warfare techniques, clearly those development efforts are not for the purpose of committing crimes under this convention, but are intended chiefly for the wartime application of IW techniques. Thus, it would seem impossible for a person, acting within the scope of a government mandate to develop IW techniques, to posses the *mens rea* necessary for this offense.

b) Computer-Related Offenses

The two computer-related offenses of computer-related forgery and computer-related fraud could also relate to the conduct of IW. Computer-related forgery is the introduction of inauthentic information into a system with the intent that it be regarded as authentic.[136] Computer-related fraud is similar. It encompasses the causing of a loss of property by means of manipulating computer data or the functioning of a computer system.[137] This type of activity could be conducted in the IW context by manipulating the banking records of opposition leaders or terrorist

---

[135] *Ibid.* at Article 6.
[136] *Ibid.* at Article 7.
[137] *Ibid.* at Article 8.

groups and their front organizations. Again, these provisions should be given serious consideration before the implementation of such techniques, especially absent a state of armed conflict.

c) Law Enforcement Inquiries

While the Convention is silent on the question of whether its limits should apply to those acting on behalf of the government, it does anticipate governments gaining access to otherwise protected information in the context of criminal investigations and international cooperation in criminal investigations. Without going into the details of the provisions, states agree to adopt procedures whereby law enforcement investigators will be able to gather evidence contained in computers, computer systems and networks.[138] These specific provisions regarding access to systems by state officials raise the possibility that access outside of these provisions would be considered illegal.

d) Intelligence Gathering

Outside of the law enforcement context, espionage is the other government purpose most likely to be served by accessing and/or intercepting data contained in and moving across foreign computer networks. Espionage has occupied a rather unique position in international law. When caught, spies are generally subject to the domestic espionage laws of the country where they are acting and can be punished, or even executed in accordance with that law, unless they enjoy diplomatic immunity, in

---

[138] *Ibid.* at Articles 19-21.

which case they will be expelled as *persona non grata*.[139] Thus, it could be said that state practice has recognized spying as a method of statecraft undertaken at the peril of the individuals engaging in it. As governments and militaries become increasingly networked, cyber-espionage will undoubtedly grow concomitantly. Espionage conducted by virtual incursion into systems of another nation could, for all practical purposes, escape the risks of detention and prosecution inherent in more traditional modes of spying, since a person need never set foot in the target country to invade its systems. As one writer noted, "When one state hacks into another state's computer systems it is very likely engaging in acts that are unlawful under the domestic law of the territorial state, but under international law, the hacking state may be engaging in a lawful act of espionage that may not be considered a use of force."[140] With the advent of the Cybercrime Convention, the appellation, "lawful act of espionage," may become increasingly problematic, especially as the convention becomes more widely adhered to or other similar conventions begin to proliferate. Thus, while the wide proliferation of similar conventions represents a positive and necessary step in being able to effectively combat criminal activity that by its international character has heretofore confounded law enforcement, it will undercut the assumption that cyber-espionage can be engaged in with impunity.

---

[139] W. G. Sharp, Sr., *Cyberspace and the Use of Force*, (Falls Church VA: Aegis Research Corp., 1999) at 125-6.

[140] *Ibid.* at 126-7.

e) Jurisdiction and Extradition

The Convention not only defines offenses, it also serves as a basis for the exercise of jurisdiction over and the extradition of offenders, once found.[141] The relatively broad bases for jurisdiction and the "extradite or present" formula, if followed should provide a means for the cooperative management of cybercrime incidents between or among signatories, hopefully making unnecessary the consideration of whether a threat or use of force would be necessitated. It provides a means by which a state can manifest its lack of acquiescence in the terrorist acts of those operating within its borders. Furthermore, the level of cooperation envisioned by the Convention, would decrease the likelihood or the perceived need for a state to intervene without the consent of a co-signatory. On the other hand, states must take care in developing IW doctrine for military operations other than war, lest they find themselves in the embarrassing situation of being called upon by a co-signatory to extradite members of their armed forces for acts committed in the performance of their duties.

E. U.S. Law Regarding Military Response to Criminal Acts

Under U.S. domestic law, it is a criminal offense to use military forces as, "a posse comitatus or otherwise to execute the laws...."[142] Though moderate exceptions have been made to allow for the provision of assistance to drug interdiction efforts,

---

[141] *Cybercrime Convention*, *supra* note 1, at Articles 22, 24.
[142] 18 U.S.C. § 1385.

this provision is broadly understood as a prohibition of the use of the military as an instrument of domestic law enforcement.[143] As noted above, terrorism in particular presents a situation where military and law enforcement responses may be appropriate in response to the same act. Military and law enforcement officials must, therefore, be sensitive to the interaction of posse comitatus and homeland defense. Title 10 provides more specific limitations on military involvement and also provides the basis for limited emergency exceptions.[144] Of importance to domestic pursuit of terrorists is the prohibition against direct participation in a search, seizure, arrest or similar activity.[145]

Though one might have expected a significant relaxation of the Posse Comitatus Act in response to the terrorist attacks of 11 September, such was actually not the case. The only modification made by the USA Patriot Act was the expansion of an exception related to military assistance in response to an emergency situation involving a weapon of mass destruction.[146] The provision, which previously limited assistance to incidents involving chemical or biological weapons, was expanded to apply to all weapons of mass destruction.[147]

The Posse Comitatus Act confirms in a broad sense that which is implicit in the Cybercrime Convention, that the primary response to criminal activity should be a law enforcement response. By providing for a more effective means of international law enforcement, the perceived need for a military response should be lessened. This

---

[143] See 10 U.S.C.A. § 374 (West Supp. 2002).
[144] See 10 U.S.C. §§ 371-382.
[145] 10 U.S.C. § 375.
[146] 10 U.S.C. § 382.
[147] USA Patriot Act, *supra* note 84 at § 104.

does not detract, however, from the point that a military response might become appropriate to the extent a cybercrime meets the criteria discussed above. This can only be accomplished by close cooperation and information exchange between the law enforcement and defense communities. An atmosphere of trust between the communities is the only effective assurance that the two will not be tempted to overstep their statutorily mandated areas of separation.

F. Concluding Observations on Cybercrime

This section has discussed the issues of cybercrime and cyber-terrorism, both as potential limitations on the conduct of IW activities in the absence of armed conflict and as possible bases for response by use of force. Terms such as "confidentiality, integrity and availability of computer data and systems"[148] are increasingly recognized as values worthy of protection. This protection has, of necessity, began its evolution from the domestic to the international sphere. That same necessity will likely provide the impetus for an even broader recognition of these values. As these values acquire increasing normative relevance, their violation by governments, especially during peacetime, should be expected to meet with increasing levels of international disfavor.

By taking a cautious approach to the peacetime application of IW techniques, governments retain the credibility to legitimately claim a right of response to similar activities by other states, organizations or individuals. As critical elements of national infrastructure depend increasingly on the flow of accurate information, the

---

[148] *Cybercrime Convention*, *supra* note 1 at Chapter II, Section 1, Title 1.

potential impact of cyber-attack increases as well, to the point that attacks on this infrastructure may come to impinge upon critical national security interests in a way that will require the consideration of a military response. In the section that follows, this thesis will examine various characterizations that could be given a cyber-attack and the permissible responses that flow from those characterizations. It will attempt to distinguish between legitimate activity, intervention, use of force and armed attack and will evaluate the significance of these terms. Finally, it will discuss the limitations provided by the LOAC in situations where the use of force is seen as appropriate.

IV. Information Warfare and International Law

Having examined the circumstances under which the employment of IW techniques by civilians or organizations may be attributable to a state, it is appropriate now to turn to the question of how to characterize various possible implementations of IW and the permissible range of responses based on those characterizations. The criteria discussed herein should apply with equal force to actions taken directly by organs of state and activities otherwise imputable to a state.

This section will examine applicable rules of customary international law, treaty law and non-binding resolutions dealing with the issues of intervention, aggression and the use of force, paying particular attention to the suitability of traditionally accepted modes of defining international law in the face of the significant challenges posed by so-called "humanitarian intervention" and of the growing threat from terrorism. It will go on to examine those rules dealing with

communications media likely to be used in IW. Finally, it will discuss the factors applicable to the use of IW in a state of armed conflict.

A. Sources of International Law

International law differs from domestic law in several important ways. Unlike domestic law, where the citizenry is governed by rules promulgated by a sovereign government possessed of enforcement mechanisms capable (at least in theory) of exacting compliance, international law is premised on agreement among sovereign equals. A fundamental precept of International Law, derived from the *Steamship Lotus* case recognizes that which is not specifically prohibited is permitted.[149] The Statute of the International Court of Justice sets forth four sources that the Court should use in applying international law. They are widely referred to as 1) "law-making" conventions, 2) custom, 3) general principles of law and 4) judicial decisions and teaching of "highly qualified publicists."[150] The fourth category is not a source of law as such, but is instead, a "subsidiary means for the determination of rules of law."[151] This is further clarified by Article 59 of the Statute, which renders decisions of the International Court binding only on the parties to the case.[152] According to Brownlie, this provision was intended to "rule out a system of binding precedent."[153] Thus, while decisions of the Court will often carry great persuasive weight, the rule of

---

[149] *Steamship Lotus Case (France v. Turkey)* (1927), P.C.I.J. (Ser. A) No. 10 at 18-19.

[150] *Statute of the International Court of Justice*, 26 June 1945, 59 Stat. 1031 [hereinafter *ICJ Statute*] at Article 32; I. Brownlie, *Principles of Public International Law,* (5th ed.) (Oxford: Clarendon Press, 1998) at 1-30 [hereinafter Brownlie, *Principles*].

[151] *ICJ Statute*, *Ibid.* at Article 32(d).

[152] *Ibid.* at Article 59.

[153] Brownlie, *Principles*, *supra* note 150 at 21.

stare decicis, typical of common law jurisprudence, does not apply in the context of international tribunals.

The Restatement Third of the Foreign Relations Law of the United States uses slightly different terminology in listing the first three as sources of International Law. It identifies customary law, international agreement and "derivation from general principles common to the major legal systems of the world."[154] The term, "general principles" has largely been applied in the procedural context, as state practice provides no guidance for the operation of such entities as international tribunals. Thus, "What has happened is that international tribunals have employed elements of legal reasoning and private law analogies in order to make the law of nations a viable system for application in a judicial process."[155] By operation of this rule, courts have been able to apply such principles as estoppel, acquiescence, *res judicata* and circumstantial evidence even in the absence of pre-existing state practice or international agreement.[156] Beyond the procedural context, certain substantive rules have been recognized as part of the *jus cogens* (also referred to as peremptory norms), a body of customary law that has become so widely accepted that its rules are regarded as general principles, which cannot be modified by subsequent treaty or agreement but only by a subsequent customary rule.[157] Article 2(4) of the U.N. Charter is often cited as such a peremptory norm.[158] The *jus cogens* thus possesses elements of both custom and general principles. Given the largely procedural

---

[154] *Restatement (Third) of the Foreign Relations Law of the United States* (1987) [hereinafter: *Restatement*] at § 100.

[155] Brownlie Principles, *supra* note 150 at 16.

[156] *Ibid.* at 17-18.

[157] *Ibid.* at 19, 513.

[158] *Restatement, supra* note 160 at § 121, comment k.

application of "general principles" and the subsidiary classification of judicial decisions and learned writings, it is clear that the primary sources of substantive international law are customary international law and treaty law.

1. Customary International Law

A significant source of international law is to be found in international custom. The Statute of the International Court refers to custom as "general practice accepted as law."[159] The Restatement uses similar terms: "general and consistent practice of states followed by them from a sense of legal obligation."[160] These definitions highlight the two requirements for a custom to be considered part of customary international law. Those requirements are state practice and *opinio juris sive necessitatis* (or simply *opinio juris*).[161] A significant aspect that distinguishes rules of customary international law from treaty obligations is the fact that the former apply to all states, as opposed to the latter, which derive their authority from a state's choice to be bound by them.[162] Certain customary rules may be considered to have become peremptory norms or *jus cogens*. These are rules from which no derogation is allowed and which cannot be changed except on the emergence of a new peremptory norm.

---

[159] *ICJ Statute*, *supra* note 150 at Article 38(b).
[160] *Restatement, supra* note 160 at § 102(2).
[161] *Nicaragua Case*, *supra* note 105, at 97.
[162] See Brownlie, *Principles*, *supra* note 150 at 10, discussing the exception to this general principle presented by the "persistent objector." Brownlie notes, "Evidence of objection must be clear and there is probably a presumption of acceptance which is to be rebutted."

a) State Practice

Some debate surrounds the questions of how widespread a particular practice must be and over what period of time it must be observed to merit consideration as a norm of customary international law. It is generally recognized that no particular time frame is necessary, but that a history of usage will provide strong evidence of the necessary "consistency and generality of practice" to meet this criterion.[163] In terms of consistency, complete unanimity of practice is not required, but there must be at least "substantial unanimity."[164] Furthermore, there must me a representation of states with a special interest in the matter.[165] The true task of interpretation is determining whether acts inconsistent with a purported custom should be treated as breaches of the custom or evidence of its non-existence or repudiation.[166]

b) *Opinio Juris*

As the Restatement notes, "a practice that is generally followed but which states feel legally free to disregard does not contribute to customary law."[167] The secondary sources referenced in Article 38(d) of the ICJ Statute are important in determining the existence of a practice, but are of even greater significance in examining the question of *opinio juris*. As Professor Brownlie observed, "In many cases the Court is willing to assume the existence of an *opinio juris* on the basis of evidence of a general practice, or a consensus in the literature, or the previous

---

[163] Brownlie, *Principles, supra* note 150 at 5.
[164] *Ibid.*; *Asylum Case(Columbia v. Peru)*, [1950] I.C.J. Rep. 266 at 276-7; *Nicaragua Case, supra* note 105 at 98.
[165] *North Sea Continental Shelf Case,* [1969] I.C.J. Rep. 3 at para. 73.
[166] *Nicaragua Case, supra* note 105 at 98.
[167] *Restatement, supra* note 160 at § 102, comment c.

determinations of the Court or other international tribunals."[168] The *Nicaragua* case was decided almost exclusively on the basis of customary international law. In that case, the Court relied heavily on United Nations General Assembly resolutions and in particular on UNGA Resolution 2625, the so-called Friendly Relations resolution, in concluding that customary international law prohibits both the use of force in international relations and the intervention in the internal affairs of other nations.[169]

2. Treaty Law

Many treaties purport to create binding norms governing the future conduct of the parties. These treaties, referred to as "law making" treaties create rules of law binding on their parties, at least in their relations with one another.[170] Many broad-based conventions applicable to the present inquiry are of this type, including the Hague Conventions of 1899 and 1907 dealing with the law of war, the Geneva Conventions of 1949, and various protocols thereto, dealing again with the law of war, and those portions of the U.N. Charter setting forth rules to be followed by states in their international relations.[171] Treaties, or portions thereof, may attain such widespread acceptance and usage that their provisions become binding on all nations as a part of the customary international law. In such a circumstance, the custom takes on an identity separate from the treaty obligation, such that the renunciation of the

---

[168] Brownlie, *Principles*, *supra* note 150 at 7 (references omitted).
[169] *Nicaragua Case*, *supra* note 105 at 99-100.
[170] Brownlie, *Principles*, *supra* note 150 at 12.
[171] *Ibid.*

treaty will likely not be sufficient to terminate the application of the customary rule.[172]

3. Resolutions of International Governmental Organizations

Resolutions of the United Nations General Assembly, of organs of the U.N. or of other international bodies are generally not considered binding on nations. They may, however, state principles of customary international law or serve as the basis for the more expeditious adoption of a rule of international law. Thus, one must generally look to the circumstances surrounding the adoption of a resolution, the extent to which it is followed in practice and its stated purposes to ascertain what weight should be given to a particular enactment.[173] Thus, a unanimously adopted resolution purporting to state principles of international law would be a stronger candidate for inclusion in customary international law than a similar resolution adopted with significant dissenting votes and abstentions.

One international body that merits separate treatment is the International Law Commission (ILC). As the organ of the U.N. responsible for the codification and progressive development of International Law, principles put forth by the ILC leave little ambiguity as to their purpose. While the circumstances of adoption and subsequent state practice may still negate any inference that an ILC pronouncement has enunciated rules of customary international law, these instruments may provide a

---

[172] *Ibid.* at 13.
[173] *Ibid.* at 15.

basis for more rapid recognition of a customary norm or as the impetus for the subsequent adoption of a binding treaty.[174]

B. IW and Levels of Coercion

In international relations, the lawfulness of various forms of coercion among states is of prime importance. It is clear from the definitions of IW, that its implementation will necessarily involve differing levels of coercion. The question of the lawfulness of a particular implementation of IW will depend in large measure upon how it is to be characterized. As already mentioned, the *jus ad bellum* is concerned with the lawfulness of the use of force. Accordingly, a threshold question in analyzing a particular proposed use of information warfare is whether such use amounts to a use of force. The question remains to be answered whether this concept will remain moored to its traditional understanding as the use of physical force against a sovereign state or will of necessity expand to encompass electronic incursions into the information infrastructure of an adversary state or it's armed forces.

C. Approaches to Coercion in International Law

The Charter of the United Nations is the beginning and ending point of any inquiry into coercion among states. The primary prohibition is found in Article 2(4) of the Charter, which provides:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political

---

[174] *Ibid.* at 30.

> independence of any state, or in any other manner inconsistent with the Purposes of the United Nations. [175]

Chapter VII of the Charter allows for collective or individual coercive responses to "Threats to the Peace, Breaches of the Peace, and Acts of Aggression" when authorized by the Security Council.[176] Articles 41 and 42 make clear that the Security Council may authorize coercive measures up to and including the use of armed force.

A further exception to the Article 2(4) prohibition on the use of force is found in Article 51, which provides, "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...."[177] Thus, the Charter provides a prohibition against the threat or use of force except in the case of Security Council approval or self-defense.

The so-called "Non-intervention principle" is an outgrowth of Article 2(7), which provides, "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state...."[178] This principle and the non-use of force principle have been the subject of various attempts at elaboration through General Assembly resolutions, ICJ decisions and scholarly writings. These elaborations can broadly be classified into two camps. On the one hand are those strictly interpreting the Charter prohibitions and the customary rules of international law that have arguably grown out of them. On the other hand are those advocating a more flexible application of these

---

[175] U.N. Charter, Article 2(4).
[176] *Ibid* at Article 39.
[177] *Ibid* at Article 51.
[178] B. Simma, Ed., *The Charter of the United Nations: A Commentary* (Oxford: Oxford University Press, 1994) at 139.

instruments in order to accomplish their underlying purposes. In either case, the task most often involves determining the proper interplay between state sovereignty and other widely recognized community values.

1. Various Forms of Coercion

Though use of force has been widely addressed in the literature, it is not the only form of coercion exercised among states. It has been said, "If all you have is a hammer, everything looks like a nail." Exclusive focus on the question of the use of force ignores the possibility that a particular operation, while not rising to the level of a prohibited use of force, may run afoul of other well-recognized principles of international law and may contravene important community values. In more closely examining other international norms and community values underlying the proscription on intervention, one may develop a more meaningful and comprehensive frame of reference, better suited to analysis of IW and its methodologies.

Thus, this thesis will focus on the question of intervention as the appropriate frame of reference. Intervention is here envisioned in a broader context that includes, but is not limited to, the application of force. In Professor Teson's book on humanitarian intervention, he provided a helpful breakdown into three categories, "Soft, Hard and Forceful Intervention."[179] Soft intervention refers to "discussion, examination, and recommendatory action."[180] Due to their non-coercive nature, these types of measures are generally considered not to fall within the category of internationally prohibited acts. Hard intervention, on the other hand, refers to

---

[179] F. R. Teson, *Humanitarian Intervention: An Inquiry Into Law and Morality* 2nd ed., (Irvington-on-Hudson, NY: Transnational Publishers, Inc., 1997) at 133.

[180] *Ibid.* at 135.

measures falling short of the use of force that are nonetheless coercive in nature such as economic sanctions.[181] Considering the finding of the ICJ that certain types of activities on the economic plane do not constitute an unlawful intervention,[182] the category of hard intervention may be seen as consisting of measures that may be *prima facie* either lawful or unlawful absent some kind of justification. Finally, forcible intervention refers to those interventions that constitute a use of force in the conventional sense.[183] Given the overlap between the concepts of intervention and use of force, those measures that justify a use of force (particularly an armed attack giving rise to a right of self-defense), would obviously justify interventions short of the use of force as well. For that reason, the use of force will be discussed herein as a subset of intervention and will only be separately discussed where different rules or values pertain. Thus, this section will examine the question left unanswered by Lt Col Schmitt's thoughtful analysis of computer network attack in terms of a "use of force" paradigm.[184] It will focus on the values that underlie the prohibition and seek to distinguish between the settled and the controversial.

2. IW as an Intervention

Several U.N. General Assembly Resolutions and the *Nicaragua* case suggest that a level of internationally prohibited intervention in the affairs of other states exists in addition to the prohibition found in Article 2(4) of the Charter against the

---

[181] *Ibid.*

[182] *Nicaragua Case, supra* note 105 at 126.

[183] Teson, *supra* note 179 at 135.

[184] See M. N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" (1999) 37 Colum. J. Transant'l L. 885 at 923. This article provides an excellent analysis of the how the use of force analysis may be applied to IW and is particularly useful in addressing the question of when a use of IW (specifically a computer network attack) could be deemed an armed attack justifying a response by conventional, forceful means.

threat or use of force. No multi-lateral, law-making treaty has further defined this "non-intervention" principle. It is, however, considered a corollary of the principle of the independence and equality of states.[185] As such, the principle is widely accepted, notwithstanding disagreements among states and scholars on its limitations and its application.

3. Intervention and Friendly Relations

The *Nicaragua* case found a customary international law norm prohibiting intervention in the internal affairs of other states, relying largely upon the 1970 Principles of International Law Concerning Friendly Relations and Co-operation Among States, adopted pursuant to Resolution 2625 of the U.N. General Assembly.[186] The ICJ's methodology in finding the required state practice and *opinio juris* for determining the existence of a rule of customary international law has been criticized for its relatively cursory treatment of the wealth of state practice contrary to the principles stated therein and its findings regarding state practice.[187] Nonetheless, the literature and state practice since the *Nicaragua* case suggest that the general principle is widely accepted. The debate has centered more on its limits than on its existence, with states not generally claiming an unlimited right of intervention, but instead articulating some basis of justification for acts that would be seen as

---

[185] Brownlie, *Principles*, *supra* note 150 at 293.

[186] *Nicaragua case*, *supra* note 105 at 100, citing *Declaration on Friendly Relations*, *supra* note 100.

[187] See e.g. T.N. Franck, "Appraisals Of The ICJ's Decision: Nicaragua V. United States (Merits)" (1987) 81 A.J.I.L. 116 at 118, F. L. Morison, "Appraisals Of The ICJ's Decision: Nicaragua V. United States (Merits)" (1987) 81 A.J.I.L. 160 at 161, Schmitt, *supra* note 184 at 920; A. D'Amato, "Trashing Customary International Law" (1987) 81 A.J.I.L. 101; Simma, *supra* note 178 at 126.

intervention.[188] Thus, the reasoning of the *Nicaragua* case notwithstanding, the Declaration on Friendly Relations is widely regarded as embodying statements of customary international law. As Professor Schachter wrote, "it has become the international lawyer's favorite example of an authoritative UN resolution."[189] In fact, it is widely regarded as an elaboration of the U.N. Charter.

This being the case, in looking at intervention, the important questions to be asked are: what are the relevant and generally agreed principles, where are the areas of ongoing debate, and what, if anything, will justify an otherwise unlawful intervention? The obvious starting place for such an inquiry is the 1970 U.N. Declaration on Friendly Relations. The draft resolution with the declaration annexed thereto was co-sponsored by 64 states and passed in the Sixth (Legal) Committee without objection on 28 September 1970. It was thereafter adopted by consensus without vote by the General Assembly on 24 October 1970.[190] The particular principle dealing with intervention recognized, "The duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter."[191] It goes on to declare, "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." [192]

Though the non-intervention principle has largely been applied to instances of assistance to armed resistance movements, it is worth noting that the text of the

---

[188] Gray, *supra* note 91 at 52.
[189] O. Schachter, "United Nations Law" (1994) 88 A.J.I.L. 1 at 3.
[190] "Principles Of International Law Concerning Friendly Relations And Co Operation Among States" in *Yearbook of the United Nations* (New York: United Nations, 1970) at 787.
[191] *Declaration on Friendly Relations*, *supra* note 100.
[192] *Ibid.*

resolution does not so limit itself. One explanation for this is the fact that states typically attempt to justify physical incursions beyond the borders of another state under the "use of force" paradigm discussed *infra*, as this paradigm is well suited to the analysis of such incursions. One of the difficulties attendant to applying a "use of force" analysis to IW is the fact that it may be employed without physically breaching a border. Much like providing funds or other forms of assistance to an armed opposition, IW is a method of causing adverse effects in another country without necessarily physically going there.

The Declaration provides a panorama of activities that amount to unlawful intervention. This list includes in addition to armed intervention, "all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements...."[193] More specific examples include "economic, political or any other type of measures to coerce another state...." The coercion here mentioned is declared unlawful if it is done to subordinate the exercise by a state of its sovereign rights and to "secure from it advantages of any kind."[194] These provisions prompt two observations. First, it is clear that the term, "armed intervention," indicates an area of overlap between the prohibition of the use of force and the non-intervention principle. Second, however, it is clear that the non-intervention principle encompasses a significantly broader array of interferences in the affairs of another nation.

At first blush, these provisions seem to prohibit many of the activities conducted by states on a fairly regular basis under the aegis of trade policy or other

---

[193] *Ibid.*
[194] *Ibid.*

forms of international relations. One task of the ICJ in the *Nicaragua* case was in differentiating between certain legal exercises of statecraft and unlawful intervention. Nicaragua contended that one way in which the U.S. committed an unlawful intervention in its internal affairs was by economic actions including the cessation of economic assistance, the reduction of sugar importation quotas and a trade embargo. While providing little analysis, the ICJ held, "At this point, the Court has merely to say that it is unable to regard such action on the economic plane as is here complained of as a breach of the customary-law principle of non-intervention."[195] On the other hand, the Court found that in providing funds, training, weapons, intelligence and logistic support, the U.S. engaged in "a clear breach of the principle of non-intervention."[196] Thus, while the principle is quite broad, the ICJ declined to apply it as broadly as the far-reaching nature of the declaration's language would suggest. In light of the general tenor of the *Nicaragua* case, placing extreme importance on the value of state sovereignty, this exclusion is certainly significant.

More important than the particular acts mentioned in the case are the characteristics of these acts that caused them to be considered an unlawful intervention. In this connection, the wording of the declaration relating to the purposes of an intervention becomes important. The act must be done in order to limit the state's exercise of its sovereign rights and to secure certain advantages.[197] The ICJ's focus on these provisions seems to be a tacit rejection of the sweeping

---

[195] *Nicaragua case*, *supra* note 105 at 126.
[196] *Ibid.* at 124.
[197] *Ibid.* at 101.

wording of the Declaration prohibiting intervention "for any reason whatever."[198] This wording instead allows for substantial interpretive latitude regarding exactly what are a state's sovereign rights. For instance, in the context of the *Nicaragua* case, what one may see as Nicaragua's right "freely to choose and develop its political, social, economic and cultural systems,"[199] another might see as the systematic, totalitarian abuse by the Nicaraguan government of the human rights of its nationals.[200] The ICJ's decision is predicated on its adoption of the former view. Adherents to either view would likely agree, however, that there seems to be general consensus that it is unlawful to intervene in the affairs of another state in a manner that interferes with that state's rightful exercise of its sovereignty. While there may still be debate on the extent of that sovereignty, particularly when it is exercised in a manner resulting in violations of widely accepted humanitarian norms, the basic premise seems well established.

4. Possible Justifications for Intervention

While the existence of the prohibition on intervention is widely accepted in principle, its application has proven much more controversial. While many nations seem to hold to a rather absolutist interpretation of the principle, others have enunciated various justifications for acts that seem *prima facie* to be violations. From hostage rescue operations and responses to terrorist attacks to the intervention by NATO in the former Yugoslavia on humanitarian grounds, the concept of absolute

---

[198] *Declaration on Friendly Relations*, *supra* note 100.

[199] *Ibid.*

[200] See generally F.R. Teson, "Appraisals Of The ICJ's Decision: Nicaragua V. United States (Merits)" (1987) 81 A.J.I.L. 173.

state sovereignty is increasingly being subordinated to other, often conflicting, norms, sometimes by individual states and at other times by groups of states.

a) Chapter VII Authorization

The Friendly Relations Resolution itself provides a potentially significant limitation when it notes, "Nothing in the foregoing paragraphs shall be construed as affecting the relevant provisions of the Charter relating to the maintenance of international peace and security."[201] This is a reference to Chapter VII, and particularly Article 39 of the U.N. Charter, vesting in the Security Council, the duty to determine the type of collective measures necessary to "maintain or restore international peace and security."[202] This is significant in that the threshold for Security Council Action under Chapter VII is much lower than that for an individual state's use of force. The Security Council can act based on a "threat to the peace, breach of the peace, or act of aggression."[203] Furthermore, the Security Council is afforded wide latitude in deciding whether such a threat or breach has occurred.[204] Articles 41 and 42 clarify that peaceful and/or forceful means of quelling such a threat or breach are permissible when authorized by the Security Council. One cannot therefore underestimate the potential importance of Security Council approval in legitimizing otherwise questionable activities.

---

[201] *Declaration on Friendly Relations, supra* note 100.
[202] U.N. Charter, Article 39.
[203] *Ibid.*
[204] Schmitt, *supra* note 184 at note 112.

b) Invitation

A state's exercise of its sovereignty is, of course, not undermined by an intervention that takes place at its invitation. It is generally understood that intervention is appropriate at the invitation of a government, but not at the invitation of those seeking to overthrow the government, as any other interpretation would render the entire concept of non-intervention meaningless. Again, conflict has arisen, not as to the principle, but as to its application. While the ICJ recognized a general right for a nation to ask for assistance, it decided against the U.S. contention that it was acting in collective self-defense of El Salvador on the basis of its factual finding that there was no credible contemporaneous request for such assistance by El Salvador.[205] On other occasions, questions have concerned which group is the legitimate government, possessed of the right to request assistance or the reality of particular purported requests for assistance, but these instances have served to show a general understanding by nations of the legal effect of invitation as a basis for intervention.[206]

c) Self-Help

In the *Corfu Channel* case, the British claimed a right to enter Albanian territorial waters for the purposes of gathering evidence of unlawful mine laying on the part of Albania to present to the ICJ. While the Court found that Albania was indeed responsible for the mine laying, it found the British intervention an unjustified violation of Albanian sovereignty despite Albania's "complete failure to carry out its

---

[205] *Nicaragua case*, *supra* note 105 at 120.
[206] See generally Gray, *supra* note 91 at 60-78.

duties after the explosions, and the dilatory nature of its diplomatic notes."[207] The Court gave precedence to Albanian sovereignty over the need to effectively gather evidence and in so doing declined to recognize a doctrine of intervention as a form of self-help. Its decision is summed up in the oft-quoted passage:

> The Court can only regard the alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to most serious abuses and such as cannot, whatever be the present defects in international organization, find a place in international law. Intervention is perhaps still less admissible in the particular form it would take here; for, from the nature of things, it would be reserved for the most powerful States, and might easily lead to perverting the administration of international justice itself.[208]

d) Proportionate Countermeasures

The Nicaragua case acknowledged the possibility that an intervention not rising to the level of an armed attack might nonetheless justify countermeasures short of a use of force that might otherwise constitute an unlawful intervention. Though the statement was not necessary to the decision of the case, given the Court's determination that the U.S. had engaged in a use of force, the Court nonetheless, without explanation or analysis opined that such a right to proportionate counter measures is vested only in the state which was the victim of the initial intervention.[209] If this is to be understood as a repudiation of the concept of invitation discussed previously, such repudiation has not taken root in subsequent state practice or writings.

The ILC Draft Rules on the Responsibility of States also clearly recognize a right to employ countermeasures against a state found responsible for an international

---

[207] *The Corfu Channel Case (Merits),* [1949] I.C.J. Rep. 4 at 35.
[208] *Ibid.*
[209] *Nicaragua case, supra* note 105 at 127.

wrong.[210] The draft rules allow for countermeasure consisting of non-performance of international obligations owed the offending state, but do not excuse the obligation to refrain from the threat or use of force or to observe basic human rights.[211] Furthermore, the countermeasures must be proportionate to the wrong done.[212] As mentioned earlier, the artificial notice and negotiation requirements envisioned as a pre-requisite to the employment of countermeasures is subject to criticism and is unlikely to garner widespread support.[213] Nonetheless, it seems well established that the breach of an international obligation does give rise to a right to resort to proportionate, non-forceful countermeasures. The rule of proportionality and political reality should appropriately focus the countermeasures on bringing an end to the wrong and not on mere punitive retribution.

e) Article 51 and Self-Defense

The inherent right of self-defense against an armed attack is by far the most frequently invoked and widely accepted justification for the use of force in international relations. Article 51 of the Charter memorialized this right, which has been recognized as the customary corollary of the prohibition on the use of force.[214] Though self-defense is largely discussed as a justification for the use of force, it could not be reasonably argued that it does not also justify less coercive means of intervention. To hold otherwise would result in a rule requiring a nation to use force when a non-forceful alternative was available. Thus, while this subsection will

---

[210] ILC Draft Rules, *supra* note 92 at Part III.
[211] *Ibid.*at Articles 49(2), 50.
[212] *Ibid.* at Article 51.
[213] See *supra* Section III.B.1.a).
[214] *Nicaragua case*, *supra* note 105 at 102.

discuss the use of force, it should be seen as equally applicable to non-forceful intervention.

(1) Individual or Collective Self-defense

Traditionalists, relying on a literal reading of Article 51, limit the right of self-defense to a proportionate response to an armed attack that has already occurred.[215] This baseline has traditionally represented the easiest question, but the answer to the question of what constitutes an armed attack has not always been as obvious as it may seem at first blush. The ICJ adopted the 1974 Definition of Aggression annexed to General Assembly Resolution 3314(XXIX) as a standard for defining an armed attack. The definition thus included, "not merely action by regular armed forces across an international border, but also 'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (*inter alia*) an actual armed attack conducted by regular forces, 'or its substantial involvement therein.'"[216] On the other hand, the ICJ held, "[T]he Court is unable to consider that, in customary international law, the provision of arms to the opposition in another State constitutes an armed attack on that State."[217]

In the IW context, it has been said that a computer attack would only constitute an armed attack when, "it is intended to directly cause physical destruction or injury."[218] Stated another way, "[A]n armed attack may occur when a use of force

---

[215] Brownlie, *Use of Force, supra* note 103 at 272-4.
[216] *Nicaragua case, supra* note 105 at 103.
[217] *Ibid.* at 119.
[218] Schmitt, *supra* note 184 at 929.

or an activity not traditionally considered an armed attack is used in such a way that it becomes tantamount in effect to an armed attack."[219]

The Charter, at least as understood by traditionalists, provides two temporal limitations on the unilateral or collective use of force. As mentioned above, the right to initiate force is conditioned upon the occurrence of an armed attack. Additionally, the right to use force, under a strict interpretation of Article 51, continues only "until the Security Council has taken the measures necessary to maintain international peace and security."[220] Thus, the unilateral use of force should be seen as a stopgap measure until such time as an effective collective response can be mounted. Again, the preference for collective action is apparent both before and after the initiation of hostilities.

(2) Anticipatory Self-Defense

A contentious issue has historically involved the question of whether the actual occurrence of an armed attack is truly a pre-cursor to the legal use of force or whether forceful action can be taken to prevent an attack when one is imminent. It is generally accepted that the customary law recognized such a right to anticipatory self-defense prior to the U.N. Charter,[221] thus the debate has centered around the question of whether the "inherent" right of self-defense recognized by Article 51 was a preservation of this existing right or the enunciation of a new, more restrictive

---

[219] Sharp, *supra* note 139at 115, analogizing from Professor Brownlie's observation that the use of weapons not involving an explosive effect such as biological or chemical weapons should nonetheless amount to an armed attack, chiefly because they are "employed for the destruction of life and property." Brownlie, *Use of Force*, *supra* note 103 at 362.

[220] U.N. Charter, Article 51.

[221] Brownlie, *Use of Force*, *supra* note 103 at 257.

standard. The classic statement of the right of anticipatory self-defense is the statement of Webster in the *Caroline* case that the right attains when, "the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation."[222] While proponents rely on the fact that to be "inherent" the right must have pre-dated the Charter, opponents argue that the wording, "if an armed attack occurs" was clearly intended to limit the pre-existing right.[223] Despite the fact that the doctrine has seldom been cited as an actual justification by states, adherents have continuously preserved the argument by assuring that more restrictive prohibitions on the right of self-defense did not make their way into General Assembly resolutions on the issue, such as the *Definition of Aggression,* the *Declaration on Friendly Relations*, or the *Declaration on the Non-Use of Force*.[224] Thus, it would appear that one could argue either that a sufficient consensus has not arisen to foreclose the right of anticipatory self-defense, or to the extent such a customary norm has developed, nations such as the United States, who have consistently supported the doctrine, have opted out of the rule as "persistent objectors."[225]

(3) Protection of Nationals, Rescue Operations

If the doctrine of anticipatory self-defense challenges the temporal limitation many would place on the right of self-defense, the issues of protection of nationals abroad and rescue operations challenge supposed territorial limits of the concept.

---

[222] Simma, *supra* note 178 at 675.
[223] *Ibid* at 676.
[224] Gray, *supra* note 91, 112.
[225] Brownlie, *Principles*, *supra* note 150 at 10.

States conducting rescue operations without the consent of the nation in which the operation takes place generally interpret Article 51 as extended to defense, not only of a state's territory, but also of its nationals abroad.[226] Debates on the issue have revealed sharp division between its proponents and opponents, preventing the Security Council from adopting a position one way or the other. Though the General Assembly has condemned U.S. interventions in Grenada and Panama, for which rescue of nationals was put forth as a justification, little can be gleaned from these resolutions in that they are not unequivocal and the rescue operations were not the only justifications put forth.[227] Thus, rescue operations would seem to be another instance where international sentiment is far from unanimous.

f) Humanitarian Intervention

It is apparent that state sovereignty is a paramount international value. In fact, it could be considered one of the cornerstone concepts underlying the U.N. system. This is underscored by the preference for collective response under Chapter VII as a prerequisite to a lawful usurpation of state sovereignty. The area of so-called "humanitarian intervention" has represented not only a significant proposed justification for intervention, but also what could be the most serious challenge to adherents of a more absolutist position regarding sovereignty.

As humanitarian law has increasingly recognized certain basic human rights as fundamental, a question that has repeatedly arisen is whether a right to so-called "humanitarian intervention" has evolved or is evolving (or has always existed) to

---

[226] Gray, *supra* note 91 at 108-9.
[227] *Ibid.*

prevent nations from systematically abusing the basic rights of its citizens under the protection of the cloak of sovereignty.

The watershed event in the discussion of humanitarian intervention is the NATO action in Kosovo. Prior to the Kosovo conflict, military action had been taken to remedy human rights abuses in Bangladesh in 1971, in Cambodia in 1978 and in Uganda in 1979, but the nations involved justified their actions as instances of self-defense, not as humanitarian interventions.[228] In the case of Bosnia, the Security Council authorized the use of force in 1995.[229] The Security Council resolutions relating to Kosovo, however, in 1998 and 1999 do not lend themselves to a meaningful interpretation allowing for NATO's use of force.[230] In providing a fundamental challenge to traditional use of force concepts, the Kosovo action necessarily speaks to the permissibility of non-forceful intervention on humanitarian grounds as well.

It is important to recognize that the contemporaneous justifications for the action in Kosovo put forth by NATO and NATO members did not assert a right of humanitarian intervention, or anything resembling a legal justification. The statements of government and NATO officials instead provided justifications more political and moral in tenor. After the fact, the use of force was justified as necessary to avert a "humanitarian catastrophe."[231] Still, a broad right of humanitarian

---

[228] *Ibid.* at 26.

[229] M. Glennon, *Limits of Law, Prerogaties of Power: Intervenionism After Kosovo* (New York: Palgrave, 2001) at 31, citing S.C. Res. 678, UN SCOR, 45th Sess., UN Doc. S/RES/678 (1990).

[230] See, S.C. Res. 1160, UN SCOR, 53rd Sess. UN Doc. S/RES/1160 (1998); S.C. Res. 1199, UNSCOR, 53rd Sess., UN Doc. S/RES/1199 (1998); and S.C. Res. 1203, UN SCOR, 53rd Sess., UN Doc. S/RES/1203 (1998).

[231] Glennon, *supra* note 229 at 24-30.

intervention was not espoused, likely to avoid "particulariz[ing] the precedent in a manner that would come back to haunt them."[232]

The Kosovo action suggests several alternative conclusions for the international lawyer. One could conclude the action, whether or not morally justifiable or necessary, is simply a violation of the U.N. Charter and customary norms against the use of force and intervention and thus should not be seen as setting a precedent. On the other hand, this could be seen as confirming the death of Article 2(4) as an effective means of governing the use of force,[233] or as Professor Sofaer has stated, the death of the "push-button" version of international law.[234] Finally, the action could be seen as confirming humanitarian intervention as an evolving exception to the prohibitions against the use of force and intervention.[235] Thus, in challenging the legal regimes relating to intervention and use of force, the Kosovo action provides a test for various schools of thought in international law. Those who see the Charter as providing relatively inflexible rules achieve a measure of clarity, but all too often at the expense of providing guidance that proves truly meaningful in the international arena. An eloquent criticism of this approach posits, "[U]nrealistic standards have made international law wholly irrelevant in use-of-force decisions."[236] State officials considering the advice of lawyers from this "push-button" camp are likely to follow the purported advice of U.S. Secretary of State, Madeline Albright, to

---

[232] *Ibid.* at 27.

[233] See Glennon, *supra* note 229, referring to T.M. Franck, "Who Killed Article 2(4)?" (1970) 64 A.J.I.L. 809.

[234] A. Sofaer, "International Law and Kosovo" (2000) 36 Stan. J Int'l L. 1 at15.

[235] For a good discussion of various interpretations, see *Ibid.* at 8-9.

[236] *Ibid* at 20.

British Foreign Secretary, Robin Cook when British legal advisers apparently opposed the Kosovo intervention: "Get new lawyers."[237]

Though adherents of the legalist camp draw support from the characterization of Article 2(4) as *jus cogens*, the rules, as enunciated by the strictest legalists are a poor predictor of actual state behavior. If one accepts as axiomatic that international law is based upon the assent of sovereign states, it is difficult to contend that states have, through treaty or custom, bound themselves to rules that would require that they be mere impotent observers of genocidal atrocities. In fact, the action in Kosovo seems to confirm that a significant number of states do not feel so constrained, at least when acting together under the auspices of NATO. While it would be difficult to argue that the basic prohibition on the use of force is not customary international law, state practice indicates that the contours of the custom are not as black-and-white as legalists believe.

In contrast to the legalists, others have noted that the wealth of practice demonstrates that international law itself is meaningless or non-existent when it comes to use of force decisions. Michael Glennon suggests that Kosovo proves once and for all that in the present political environment, international law does not and should not govern decisions on the use of force. He asserts, "The Scholastic international law rules purporting to govern intervention neither describe accurately what nations do, nor predict reliably what they will do, nor prescribe intelligently what they should do."[238] This recalls Professor Franck's lament some 30 years

---

[237] Glennon, *supra* note 229 at 178, citing J.P. Rubin, "Countdown to a Very Personal War" *The Financial Times* (30 September 2000) 9.

[238] Glennon, *Ibid.* at 204.

before, when he asked, "Who Killed Article 2(4)?"[239] Of course, the death of Article 2(4) would counter those who claim it represents *jus cogens,* but as previously noted, the *jus cogens* assertion, except in the broadest sense, is difficult to square with state practice anyway. Indeed, it is probably better for international law as a whole to concede that no law exists in a particular area than it is to claim that a rule pertains where it is violated routinely and with impunity.

The question remains, however, whether those lamenting the death of Article (2)(4) and rules against intervention are discarding the good with the bad. Put differently, even if one concedes that the more absolute prohibitions of the U.N. Charter and the Declaration on Friendly Relations do not represent norms universally agreed to, do there not remain core concepts about which sufficient consensus does exist to provide useful guidance and meaningful restraint on states' use of power solely to satisfy their national interests? There are those who would heartily answer this question in the affirmative.

g) Effective Legal Analysis Post-Kosovo

The conundrum Kosovo presents to the legalists is in actuality an affirmation of the approach long advocated by the late Professor Myres McDougal of the Yale Law School, who, with co-author Florentino Feliciano, cautioned over 40 years ago, "To seek to construct a set of words that will automatically determine all future decisions and relieve human decision-makers of the anguish of choice and judgment in responding to events of coercion and opposed claims about coercion is, of course, a

---

[239] Franck, *supra* note 233.

futile enterprise...."[240] In fact, Sofaer notes that the U.S. has traditionally followed a more flexible "common lawyer" approach in its foreign relations decisions, in which international law serves the Charter's purposes by, "guid[ing] statesmen to the issues and values they should consider as they decide whether to threaten or use force, and thereby give the law new meaning."[241] This approach is, of course, subject to criticism because of its malleability,[242] but its reference back to values enshrined in the Charter provide a sufficient ground of common understanding and meaningful self restraint, especially as a useful alternative to slavish adherence to inflexible, impractical rules. Under this approach, the international lawyer's task is not to find rules of law, but to find "issues and values" that are widely held and relate to the decision to resort to coercion at the level of intervention or the use of force. McDougal and Feliciano propose several relevant factors, roughly paraphrased below:

a. The chronological factor (who was first to engage in coercion).

b. The purpose of the coercion.

c. The type and intensity of the coercion.

d. The likelihood of escalation.

e. Proportionality of responsive coercion.

f. Effectiveness of community intervention.

g. The type and purpose of the decision required (recognizing that different standards may apply to a split-second

---

[240] M.S. McDougal & F.P. Feliciano, *Law and Minimum World Public Order: The Legal Regulation of International Coercion* (New Haven: Yale University Press, 1961).

[241] Sofaer, *supra* note 234 at 20-21.

[242] *Ibid.* at 16. See generally Glennon, *supra* note 229.

decision in the face of an immediate threat than to a post hoc determination allowing for fuller deliberation).

h. The probable effectiveness and costs of decision.

i. The anticipated impact on the values of the system of world public order.[243]

In applying such a formula to Kosovo, Sofaer concluded it was possible to legally justify the NATO intervention. He observed several justifying factors such as the violation by the Federal Republic of Yugoslavia (FRY) of universally accepted legal precepts, the scale of the killing of civilians, the failure of the FRY to respond to Security Council actions demanding cessation, the conclusion by NATO that a threat to European security existed, the prior actions by the FRY in Bosnia and several other factors.[244] In evaluating the factors, one could easily conclude that the failure of NATO to act would have been more destructive of community values than the intervention; a fact implicitly admitted by those who claim the action was illegal but justifiable.

h) Preemptive Intervention

If Kosovo showed that the traditional approach to international law was ill-equipped to halt large-scale humanitarian abuses, the future could pose even greater challenges. To say that on 11 September 2001 the assumptions the World woke up with were irreversibly altered by the time it went to sleep that night is not overly melodramatic. The World community found itself faced with an enemy for whom concepts like humanity, proportionality, sovereignty and the rule of law are

---

[243] McDougal & Feliciano, *supra* note 240 at 65-66.
[244] Sofaer, *supra* note 234 at 15.

meaningless. This fact leaves hard choices for those left with the task of responding. With the possibility of the use of weapons of mass destruction, decision-makers must strike a balance that does not hinder the ability to put a stop to the lawlessness and that also resists the temptation to sink to the same level of lawlessness, with the ultimate value, survival, hanging in the balance. In this context, Professor McDougal's warning that the mere words of the Charter should not be expected to relieve decision-makers of these hard decisions take on a prophetic ring.

In this context, many are understandably concerned that the U.S. is considering what may be the appropriate standards for pre-emptive action against terrorists and those who equip and provide safe haven to them.[245] Though the justification for the action in Afghanistan has been previously addressed, the question remains whether, once flushed out of Afghanistan, those bent on the destruction of Western values will be allowed to regroup and plan even more destructive attacks, secure behind the veil of the sovereignty of a state sympathetic to them or unable to repel them. A legalist school of thought that answers, "Yes" to this question, consigns itself immediately to the scrap heap of irrelevancy. The current situation seems to justify the conclusion that, to remain relevant, public international law on the use of force and intervention will, of necessity, have to embrace the multi-factoral value analysis discussed herein. In that context, international law can still provide the sort of meaningful restraint called for in a New York Times editorial that observes,

---

[245] "Yet the war on terror will not be won on the defensive. We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge." Office of the President of the United States, "Remarks of the President at 2002 Graduation Exercise of the United States Military Academy" 1 June 2002, online: White House Home Page <http://www.whitehouse.gov/news/releases/2002/06/20020601-3.html> (date accessed: 3 July 2002). See also D.E. Sanger, "Bush to Formalize a Defense Policy of Hitting First" *The New York Times [Late Edition]* (17 June 2002) A1.

"[T]he United States must take care not to set a dangerous example that might, say, tempt India to launch its own pre-emptive strike against Pakistan."[246]

5. Defining Community Values

While the entreaty to weigh community values might seem presumptuous, it is an undertaking that the international lawyer is perhaps uniquely suited to shoulder. One need only recall the Crusades or the Spanish Inquisition to observe the potentially devastating effect of the pursuit by one group of its values to the exclusion of those of others. A further danger inherent in a value-based system is the potential that emotional catch-phrases like "Humanitarian Catastrophe" or "Terrorism" will become subterfuges that states will use to nominally justify action actually destructive of community values. Of course, subterfuge and fanciful attempts at fitting actions within acceptable classification are no strangers to the legalist school of thought either. In fact, it could be said that inflexible rules invite even more fanciful machinations by requiring that everything fit within a set of pre-determined standards, promulgated at a time when contemporary issues were scarcely imaginable. Current information warfare capabilities were scarcely imaginable ten years ago, much less the more than 50 years since the inception of the U.N. That is not to say, however, that the Charter and subsequent agreements among nations have not enunciated common values, which should guide decision-makers with regard to IW. In looking to international agreements for common values, it is hoped one may avoid the mistakes of the past. While the U.N. Charter, the Cybercrime Convention and the

---

[246] Editorial, "Striking First," *The New York Times* (23 June 2002) D12.

consideration of the issue of terrorism have helped to illuminate certain values of varying levels of international acceptance, a look at the rules relating to the elements of the global information infrastructure should likewise yield fruitful observations about values worthy of international protection.

D. Rules Governing Transmission Media

While there has been scholarly attention paid to application of the law of armed conflict, the U.N. Charter and a collection of other broad-based international instruments to IW, there has, to date, been little analysis of the domestic and international rules related to the various media through which an IW attack could be propagated. In broad terms, land, air, sea and space can be thought of as the media through which the global information infrastructure (GII) functions. "Land" refers to the transmission of information across hard-wired networks, be they fiber optic, copper or otherwise. "Sea" regards the use of undersea transmission of information, while "Air" refers to transmission of information across the various bands of the radio frequency spectrum between land-based nodes. "Space" refers, in broad terms, to transmission to, from or through satellites. Though some would argue that the distinction between air and space is somewhat artificial given the fact that all satellite communication relies on the same radio frequency spectrum as the so-called terrestrial airwaves, the legal regime applicable to outer space is sufficiently unique to justify separate analysis.

It must be recognized that technology is rendering these divisions ever more meaningless. As one author noted, "The advent of digital technology has eroded clear lines that once existed between distinct and traditional telecommunication

services, such as radio, television, telephone, and telegraph."[247] Converging technologies have resulted in the "potential for virtually any sort of communication or information device to connect with any other."[248] Nonetheless, rules and policies have traditionally developed according to the distinct telecommunication technologies, making separate analysis still worthwhile.

1. Land

Telecommunication, in its oldest form, involves the conversion of physical input to electronic form, its transmission over conductive cables and its transmission back into a perceptible signal at the receiving end. Though the technology has improved dramatically from the telegrapher's dots and dashes sent over metallic cables to include fiber optically transmitted multi-media videoconferences, cable networks still provide the backbone of the global information infrastructure. Though the networks themselves exist within national borders, international commerce and communication have, since the days of the telegraph required some level of interconnection.

The International Telecommunications Union (ITU) has long been the preeminent body for setting international standards and policies necessary for the orderly, transnational connection of these domestic networks, though other international bodies, namely the Organization for Economic Cooperation and Development (OECD) and the World Trade Organization (WTO) have also weighed

---

[247] H.M. White, Jr. & R. Lauria, "The Impact of New Communication Technologies on International Telecommunication Law and Policy: Cyberspace and the Restructuring of the International Telecommunication Union" (1995) 32 Cal. W. L. Rev. 1 at 2.

[248] *Ibid* at 2.

in on those aspects of the GII of relevance to their missions. Thus, though states retain sovereignty over the elements of the GII existing within their borders, they have also, through membership in international organizations committed themselves to other values.

a) Universal Service and Interconnection

The values common to the missions of these international organizations, especially as they relate to telecommunication networks revolve around such phrases as "universal access," "interconnection" and "economic development." For instance, among the purposes stated in Article 1 of the ITU Constitution, a binding multi-lateral treaty, are, "to promote the extension of the benefits of the new telecommunication technologies to all the world's inhabitants," and "to promote, at the international level, the adoption of a broader approach to the issues of telecommunications in the global information economy and society...."[249]

The OECD speaks of the need to bridge the "digital divide," described as "the gap that exists between geographic areas or individuals at different socio-economic levels in respect to their opportunities to access information and communication technologies."[250] This sentiment is shared in the policy statements of the United States Agency for International Development, which launched its Internet for Economic Development (IED) Initiative in order to bridge the digital divide and "to

---

[249] *Constitution of the International Telecommunications Union,* Dec. 22, 1992, S. Treaty Doc. No. 104-34 (1996) (as amended through 1994) [hereinafter *ITU Constitution*].

[250] OECD, *OECD Communications Outlook* (Paris: OECD, 2001) at 265.

help accelerate the spread of the Internet and electronic commerce to developing nations."[251]

The WTO echoes the same chords. The Telecommunication Annex to the General Agreement on Trade in Services requires members to assure access by other member service providers to public telecommunications transport networks offered within or across its borders.[252] A large number of the WTO nations, including the U.S., have made free trade commitments under these principles. Annexed to many of these commitments, again including those of the U.S. is a "Reference Paper" stating basic agreed principles regarding regulation of telecommunications. Among the precepts contained in the Reference Paper are "interconnections" and "universal service." Thus, commitments are undertaken to assure that foreign providers are able to interconnect with domestic networks, while domestic authorities retain the ability to assure that globalization occurs in such a way as to promote universal service.[253]

While commerce and development are laudable goals, the ITU Constitution also contains protections for more basic benefits of the international telecommunication service. Article 40 provides, "International telecommunication services must give absolute priority to all telecommunications concerning safety of life at sea, on land, in the air or in outerspace, as well as to epidemiological telecommunications of exceptional urgency of the World Health Organization."

---

[251] U.S. Agency for International Development Website, online: <http://www.usaid.gov/info_technology/ied/> (date accessed: 26 June 2002).

[252] *Agreement On Telecommunications Services (Fourth Protocol To General Agreement On Trade In Services)*, March 1997, 36 I.L.M. 354 at Articles 5(a), (b), online: WTO Website <http://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm> (date accessed: 30 June 2002).

[253] "Reference Paper" 36 I.L.M. 367 (1997), online: WTO Website <http://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm> (date accessed: 30 June 2002).

b) Domestic Control

Though many nations, in the name of free trade and economic development, do provide significant levels of access to their networks, this access is not to the exclusion of important elements of national sovereignty. Thus, while the ITU Constitution, on the one hand, articulates the principle that the public should have access to the international telecommunication service, on the other hand it makes clear that nations are entitled to stop communications deemed "dangerous to the security of the state or contrary to its laws, to public order or decency" and are further entitled to the outright suspension of international telecommunications when deemed appropriate.[254] U.S. domestic legislation contains similar provisions. The U.S. Telecommunication Act enumerates "War powers of President," allowing the president to, among other things, close down or commandeer any "facility or station for wire communication" on a finding that, "there exists a state or threat of war."[255]

c) Implications for IW

This brief look at international involvement in the interconnection of domestic networks reveals overriding values that must be considered when analyzing the legality of a particular information operation. Though such values as economic development and international commerce will likely bow to national security, especially in time of war, they are considerations that should enter the calculus, especially when information operations are contemplated in conflicts short of war. For instance, the U.S. might face a credibility gap if it uses networks installed with

---

[254] ITU Constitution, *supra* note 249 at Articles 33-35.
[255] 47 U.S.C. § 606.

the assistance of the Internet for Economic Development Initiative as an avenue for information attack. On the other hand, even in the case of war, the importance of the GII to emergency medical service must be considered in weighing the proportionality of any information operation in relation to its objectives.

2. Air

With the explosion in technologies such as cellular telephone use and satellite communications, rules governing the allocation and use of the radio frequency spectrum have gained increasing importance. Again, the ITU, specifically its Radiocommunication Sector, is the primarily responsible international body.

a) ITU Constitution, Convention and Regulations

As noted above, the radio frequency spectrum is used for earth and space-based communications, creating a certain level of overlap between this subsection and subsection D. 4. below. Those rules and policies common to both sectors will be discussed in this section, while those specific to outer space will be discussed below.

(1) Non-Interference Principle

The cardinal principle governing the use of the radio frequency spectrum is the non-interference principle. To this end, one of the purposes listed in Article 1 of the ITU Constitution is to:

> effect allocation of bands of the radio-frequency spectrum, the allotment of radio frequencies and registration of radio-frequency assignments and any associated orbital positions in the geostationary-

satellite orbit in order to avoid harmful interference between radio stations of different countries.[256]

That this obligation is more than aspirational in nature is demonstrated by Article 45, which provides, "All stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members."[257] Three processes within the ITU construct achieve this non-interference. The most important of these is the allocation, through the ITU Radio Regulations, of frequency bands to particular services. For instance, cellular telephone service and satellite uplinks would be assigned different bands so that these services would not cause interference with one another. The second process, allotment, applies only to a few distinct bands and services. This process involves the allotment of particular bands to different countries, through a process known as *a priori* planning. Finally, individual states assign particular bands to their licensed radiocommunication operators. The right to protection against harmful interference arises from a state's recording of that assignment in the Master Frequency Register.[258]

The Radio Regulations and the ITU Constitution both recognize the radio spectrum as a limited national resource, to be used, "rationally, efficiently and economically."[259] Furthermore, the usefulness of radio communications in the cause of civil and rescue response is protected by Radio Regulations, which provide, "Any

---

[256] ITU Constitution, *supra* note 249 at Article 1.

[257] *Ibid.* at Article 45.

[258] See generally R. Jakhu and V. Rodriguez Serrano, "International Regulation of Radio Frequencies for Space Services" Project 2001, Group on Telecommunications (2000) at 18-22. See also International Telecommunication Union, Radio Regulations, Article S5, Footnotes S5.149, S5.341, S5.380, S5.385-88, at http://www.itu.int/brconf/wrc-2000/about/index-html (1988) ITU Radio Regulations, Articles S8.1, S11.

[259] ITU Constitution, Article 44; Radio Regulations, Article S0.3.

emission capable of causing harmful interference to distress, alarm, urgency or safety communications on the international distress and emergency frequencies ... is prohibited."[260]

(2) Applicability to Military Operations

The ITU Constitution is somewhat unique among international instruments, in that it directly addresses its impact on military operations. Article 48 provides, "Members retain their entire freedom with regard to military radio installations."[261] This absolute reservation is somewhat tempered by the following paragraph, recognizing an obligation to, "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."

(3) Implications for IW

Harmful interference is precisely the object of many IW applications, rendering such operations facially inconsistent with obligations undertaken in the ITU Constitution. However, the caveat, "so far as possible" preceding the obligation to avoid harmful interference recognizes that significant national defense interests may conflict with the non-interference principle. In this context, it is clear that the non-interference principle was not conceived of as absolute, but simply as a consideration to be given appropriate weight in the military planning process. As the intensity of conflict increases, the negative results of using interference-causing IW assets will

---

[260] Radio Regulations, Article S4.22.
[261] ITU Constitution, Article 48(1).

more likely be outweighed by such factors as minimizing collateral damage from the use of conventional weapons, and in the case of radar jamming platforms, of the safety of friendly air crews.

b) Transborder Broadcasting

Quite apart from the issue of interference is the issue of sending signals into another country for the purpose of communicating directly with a target population. This naturally results in tension between the values of sovereignty and freedom of information. As transborder radio broadcasts became ever more common, a uniform state practice of not protesting these broadcasts developed, the receiving state desiring not to prejudice its opportunities to do likewise in return. Thus, many hold that a customary norm, embodying the freedom of broadcasting emerged as early as the 1930s.[262] This general principle was limited in 1936 by the International Convention Concerning the Use of Broadcasting in the Cause of Peace, which prohibited broadcasts intended to "incite armed revolt, revolution or war or other propaganda endangering internal State security or order."[263] Another international value of relevance to IW is found in the 1948 Universal Declaration of Human Rights, a time-honored U.N. Declaration. Article 19 of that declaration provides, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold

---

[262] N.M. Matte, *Aerospace Law: Telecommunications Satellites*, (Toronto: Butterworths, 1982) at 68.

[263] *Ibid.*

opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[264]

Thus, in relation to psychological operations in particular, even in time of peace it could be said that the long-standing principle of freedom of broadcasting generally recognizes the right of one nation to broadcast messages, not falling within the prohibited categories above, into another nation. Of course, it would seem the limitations would not apply in a state of war or armed conflict, the very purpose of which is to undermine the internal security of one's adversary.

c) The Global Navigation Satellite System (GNSS) Debate

Another issue that defies ready characterization as either an air or space law issue involves the ongoing evolution of the Global Navigation Satellite System. The system, as envisioned, would integrate information from Global Positioning Satellites, communication satellites and various ground-based systems to drastically enhance aircraft navigation and air traffic management. Difficult issues face the evolution of this technology, largely arising from the fact that the only global positioning system currently seen as a likely primary signal provider for the positioning portion of the system is owned and operated by the U.S. Department of Defense. Though the signal is currently provided on a global basis, free of charge, other states are reluctant to make the substantial investment in the GNSS system,

---

[264] *Universal Declaration of Human Rights*, (United Nations 1948) (online: http://www.un.org/rights/50/decla.htm).

fearing that it could be rendered useless should the U.S. decide to degrade or discontinue the provision of the portion of the signal used by civilian systems.

(1) The U.S. Position

President Clinton, in a 1996 Presidential Decision Directive, established U.S. policy relating to GPS. The chief goals stated in that policy were strengthening and maintaining U.S. national security, on one hand, and promoting international cooperation for the use of GPS for peaceful purposes, on the other.[265] These goals are complemented by policy guidelines, which provide that the U.S. will continue to provide the signal on a worldwide basis; free of charge, but also that the system will remain responsive to the National Command Authorities.[266] Thus, while the U.S. maintains its commitment to providing the service, nations using it must realize that its use will always be subject to U.S. national security concerns. This is apparent in the regulations regarding the export of civilian band GPS receivers, which requires that they bear the proviso, "ADVISORY NOTICE: This receiver uses the GPS P-Code signal, which by U.S. policy, may be switched off without notice."[267]

(2) Non-U.S. Concerns

It is understandable that other nations are concerned about the lack of "bankable guarantees" upon which to base their decision to go forward with GNSS

---

[265] President of the United States, Presidential Decision Directive NSTC-6, (online: http://www.spacecom.af.mil/usspace/gps_support/documents/gps_pdd.htm).

[266] *Ibid.*

[267] 22 C.F.R. § 121, Category XV(c).

development.[268] Beyond considerations of cost, many states are concerned with meeting their obligations under Article 28 of the Convention on International Civil Aviation to regulate and control the provision, operation and management of air traffic management and navigation within their territories.[269] Nonetheless, the President of the Council of the International Civil Aviation Organization (ICAO), Dr. Assad Kotaite, has noted, "It has been generally agreed that there is no legal obstacle to the implementation and achievement of the CNS/ATM [Computer Navigation System/Air Traffic Management—the elements of GNSS] systems concept and that there is nothing inherent in CNS/ATM which is inconsistent with the Chicago Convention."[270] Dr. Kotaite further noted that ICAO has accepted, by exchange of letters, an offer of the U.S., through the FAA administrator, to "respect the principle of sovereignty in the provision of GPS...."[271]

(3) Implications for IW

Jamming, degrading, or just turning off the civilian band GPS signal in a given area could be in the national interest of the U.S. in a given situation. Nations who rely on this system must do so with no delusions regarding that point. From a U.S. perspective, however, many factors urge restraint in the utilization of these measures. In addition to the benefits for global development, the expansion and integration of GPS technology serves U.S. commercial interests such as shipping and

---

[268] See L. Bond, "The GNSS Safety and Sovereignty Convention of 2000 AD" (2000) 65 J. Air L. & Com. 445 at 449, quoting Attorney General Rattray of Jamaica.

[269] *Convention on International Civil Aviation*, 7 December 1944, 15 U.N.T.S. 295 [hereinafter: Chicago Convention] at Article 28.

[270] A. Kotaite, "ICAO's Role With Respect to the Institutional Arrangements and Legal Framework of Global Navigation Satellite System (GNSS) Planning and Implementation" (1996) 21 Ann. Air & Sp. L. 195 at 197.

[271] *Ibid.* at 202.

international civil aviation. Thus, action that would undermine the widespread adoption of the GNSS system, could, in the long run damage other U.S. interests. The concept of proportionality, once again provides the appropriate guideline. The ability to concentrate the effects of GPS denial to combat zones and the consideration of the effects on civilian aviation or maritime navigation should be important considerations in this regard. This fact is underscored by Article 3bis of the Chicago Convention, adopted in response to the Soviet shoot-down of a Korean Air Lines 747. That provision obliges states to "refrain from resorting to the use of weapons against civil aircraft in flight."[272] Though the U.S. has consistently refused to adhere to this protocol, it still carries persuasive weight in the international community, despite the fact that the events of September 11, 2001, may demonstrate the short-sightedness of the inflexible wording of the provision. Nonetheless, the provision highlights that the effect on civil aviation is an important consideration in planning potential information operations.

3. Sea

The oldest method for the interconnection of telecommunication systems located continents apart is the undersea cable. These cables still represent a substantial element of the GII. As such, they have long been the subject of multi-lateral treaties.

---

[272] *Protocol Relating to an Amendment to the Convention on International Civil Aviation*, 10 May 1984, 23 I.L.M. 705.

a) Submarine Cable Convention

Submarine cables have been the subject of international conventions since at least 1887.[273] With the coming into effect of the Submarine Cable Convention, damaging submarine cables intentionally or through culpable negligence was recognized as both a crime and an international delict.[274] The convention, however, clearly spelled out its non-applicability to military operations, at least at time of war by way of Article XV, which provided, "It is understood that the stipulations of this Convention shall in no wise affect the liberty of action of belligerents."[275] Thus, while submarine cables were generally protected in time of peace, they were internationally understood to be lawful targets during wartime. This understanding was refined somewhat in the Hague Convention on Land Warfare of 1907, which provided, "Submarine cables connecting an occupied territory with a neutral territory shall not be seized or destroyed except in the case of absolute necessity."[276] While not impacting the freedom of action before an occupation is affected, this rule prohibits the unnecessary and indiscriminate destruction of a vital element of the national infrastructure.

Subsequent treaties dealt with submarine cables as well. The 1958 Convention on the High Seas contained virtually identical language to the Submarine Cable Convention with respect to the offense of damaging submarine cables.[277]

---

[273] *Convention for the Protection of Submarine Cables*, 14 March 1884, 24 Stat 989 [hereinafter *Submarine Cable Convention*].

[274] *Idib.* at Article II.

[275] *Ibid.* at Article XV.

[276] *Convention (II) With Respect to the Laws and Customs of War on Land*, 29 July 1899, 32 U.S. Stat. 1803, available in Schindler & Toman, *supra* note 118 at 63, Article 54.

[277] *Convention on the High Seas*, 29 April 1958, 13 U.S.T. 2312 at Article 27.

Though this convention did not carry forward the exemption for belligerents, it did note that previous conventions between the parties remained in force, leaving the belligerent exception intact, at least as to parties to the earlier convention.[278] Though the Continental Shelf Convention, signed in conjunction with the High Seas Treaty did not contain the same provision criminalizing damage to submarine cables, it did impose a duty on coastal states not to impede the laying of submarine cables on the continental shelf.[279]

b) Law of the Sea Convention

The most comprehensive attempt at codifying the law of the sea was the United Nations Convention on the Law of the Sea (UNCLOS) of 1982. Though the U.S. has not ratified the treaty, due in large measure, to the regime created managing the exploitation of the seabed as the "common heritage of mankind," seen as antithetical to certain American ideals, other portions are seen as largely codifications of customary international law. With regard to submarine cables, the UNCLOS once again brings forward the language of the 1884 Convention criminalizing willful or culpably negligent damage to them.[280] Once again, the language relating to the activities of belligerents was not brought forward.

---

[278] *Ibid.* at Article 30.

[279] *Convention on the Continental Shelf*, 29 April 1958, 15 U.S.T. 471.

[280] *United Nations Convention on the Law of the Sea*, 10 December 1982, 1833 U.N.T.S. 3 at Article 113.

c) Implications for IW

While submarine cables have always been an important link between continental communication infrastructures, they have also historically been recognized as legitimate targets for belligerents. Physical damage to submarine cables, however, is probably now less desirable and less effective in strategic terms given the availability of other means of interconnection, via satellite and/or airwaves and given the possible utility of submarine cables as an avenue for electronic attack. Likewise, in terms of proportionality, striking at the trunk line could be seen as causing a disproportionate effect in comparison to the advantage to be gained. The actual content of the information transmitted via submarine cable has not been the subject of international agreement, likely because it is not seen as a multi-lateral issue, given that the negotiation of landing rights for submarine cables is generally a bi-lateral process and once landed, the signals are subject to domestic control.

4. Outer Space

Beyond the issues of harmful interference, largely addressed in subsection 2), *supra*, outer space is significant to IW in many ways. Communication satellites could act as the medium through which information is transmitted as part of an attack. The proliferation of space communication technology will also very likely make satellites the targets of kinetic and/or information attack. Finally, space assets could be used as a platform from which various information operations could be launched.

a) Outer Space Treaty

Any consideration of the regime of outer space must start with the 1967 Outer Space Treaty.[281] Considered by many as the "constitution of outer space,"[282] the Treaty sets forth guiding principles applicable to the exploration and use of outer space. Though the Preamble recognizes, "the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes," the term, "peaceful purposes" is not further defined in the text of the treaty.[283] Article IV, however points out that the moon and other celestial bodies are to be used for "exclusively peaceful purposes," further elaborating the complete de-militarization of the moon and celestial bodies.[284] The only other specific limitation on military operations is also contained in Article IV and prohibits the placement of weapons of mass destruction in orbit.[285]

(1) Peaceful Uses

Despite the arguably aspirational nature of the "peaceful purposes" provision of the Preamble, many countries have included the provision in their national legislation. For instance, the U.S. Congress declared, "that it is the policy of the United States that activities in space should be devoted to peaceful purposes for the

---

[281] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, 27 January 1967, 610 U.N.T.S. 205 [hereinafter *Outer Space Treaty*].

[282] I.A. Vlasic, "Some Thoughts on Negotiating and Drafting Arms Control and Disarmament Agreements Relating to Outer Space" in N.M. Matte, ed., *Arms Control and Disarmament In Outer Space: Towards A New Order Of Survival* (Montreal, Canada: Cener for Research in Air and Space Law, McGill University, 1991) 203 at 212.

[283] Outer Space Treaty, Preamble, Paragraph 2.

[284] *Ibid.* at Article IV.

[285] *Ibid.*

benefit of all mankind."[286] The meaning of the word, "peaceful," has been the subject of ongoing debate between those, including the U.S., who have maintained that it means "non-aggressive" and those, including chiefly the former U.S.S.R., who have held that it means "non-military." While this debate continued in academic circles, both the U.S. and the U.S.S.R. continued to place military satellites into orbit fulfilling missions such as reconnaissance, communication, navigation, electronic intelligence and missile launch detection, all without significant forceful protest.[287] Furthermore, various bi-lateral arms control treaties between the U.S. and the U.S.S.R. in addition to the multi-lateral Comprehensive Test Ban Treaty refer to verification by "national technical means," widely understood as a euphemism for remote sensing satellites.[288] Thus, it is difficult to deny that state practice has confirmed the U.S. interpretation of the term. In fact, in many ways military space technology has furthered international objectives such as arms control verification, civilian GPS navigation and environmental monitoring through civilianized remote sensing technology just to mention a few. Furthermore, Operation Desert Storm, referred to as "the first space war,"[289] demonstrated how space technology can ameliorate the inhumanity of war, as "smart weapons" capable of flying in the window of a military installation are certain to reduce civilian casualties.

---

[286] 42 U.S.C. § 2451.

[287] I.A. Vlasic, "Space Law and the Military Applications of Space Technology," in N. Jasentuliyana, ed., *Perspectives on International Law* (Boston: Kluwer Law International, 1995) 385 at 388 [hereinafter Vlasic, "Military Applications"].

[288] See e.g. *Treaty on the Limitation of ABM Systems and Interim Agreement and Protocol on the Limitation of Strategic Offensive Arms*, 11 I.L.M. 784 (1972) at Article XII; "Agreed Statements Annexed to SALT II Treaty" 18 I.L.M. 1112 (1979); *Treaty On Underground Nuclear Explosions For Peaceful Purposes*, 15 I.L.M. 891 (1976), Article IV; *Comprehensive Test Ban Treaty*, 35 I.L.M. 1439 (1996), Article IV.

[289] Vlasic, "Military Applications," *supra* note 287 at 388, quoting the U.S. Air Force Chief of Staff, General Merrill McPeak.

The debate has thus largely shifted from considerations of the militarization of outer space to the weaponization of outer space. Though military space technologies to date have primarily played a more passive role, enhancing the capabilities of air, land and sea forces, a U.S. Space Command vision of the future, predicts, "During the early portion of the 21st century, space power will also evolve into a separate and equal medium of warfare."[290] This is underscored by the prominence of the Space Based Laser (SBL) initiative in U.S. plans regarding ballistic missile defense.[291] Development of the SBL, seen as an important part of the "boost phase layer" of the missile defense system, is targeted to, "provide an on-orbit lethal demonstration of SBL technologies by 2012."[292] These statements, combined with the recent withdrawal of the U.S. from the Anti-Ballistic Missile Treaty,[293] signal an unmistakable move toward the placement of weapons in space in the coming decade. Given that the only hard prohibition against weapons in orbit is the Article IV prohibition relating to weapons of mass destruction, the impediments to this development are likely to be more political than legal.

(2) Common Interest, Freedom and Non-Appropriation

---

[290] U.S. Space Command, "United States Space Command Vision for 2020" February 1997, online <http://afpubs.hq.af.mil>.

[291] Ballistic Missile Defense Agency, "Fact Sheet: Space Based Laser (SBL)" (2002), online: Ballistic Missile Defense Agency Web Site <http://www.acq.osd.mil/bmdo/bmdolink/pdf/sbl.pdf> (date accessed: 3 July 2002).

[292] *Ibid.*

[293] Office of the President of the United States, Press Release "President Discusses National Missile Defense" (13 December 2001), online: White House Web Site <http://www.whitehouse.gov/news/releases/2001/12/20011213-4.html> (date accessed: 3 July 2002).

The Outer Space Treaty embodies several broad principles, generally referred to as the common interest principle, the freedom principle and the non-appropriation principle. The common interest and freedom principles are enunciated in Article I, which provides, "The exploration and use of outer space, including the moon and other celestial bodies, shall be carried our for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development and shall be the province of all mankind. Outer space ... shall be free for exploration and use by all States without discrimination of any kind...."[294] The non-appropriation principle appears in Article II, which reads, "Outer space ... is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."[295]

(3) Applicability of Public International Law in Outer Space

Another significant provision of the Outer Space Treaty is found in Article III, which provides that space activities shall be carried on, "in accordance with international law, including the Charter of the United Nations...."[296] Thus, it is clear that international law, including the U.N. provisions governing the use of force and unlawful intervention, apply with equal force to activities carried on in the outer space environment.

(4) Harmful Interference With Peaceful Uses

---

[294] *Outer Space Treaty, supra* note 281 at Article I.
[295] *Ibid.* at Article II.
[296] *Ibid.* at Article III.

Another provision of the Outer Space Treaty, found in Article IX, brings to mind the harmful interference principle found in the ITU Constitution. In addition to prohibiting the harmful contamination of outer space Article IX provides:

> If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its national in outer space ... would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space ... it shall undertake appropriate international consultations before proceeding with any such activity or experiment.

Though the obligation to enter into consultations is not as strongly stated as the ITU obligations to refrain from or cease causing harmful interference, nonetheless the basic premise of non-interference with other states in their "peaceful exploration and use of outer space," seems an undeniable corollary of Article I's freedom principle. Regardless of one's definition of "peaceful uses," by its terms, this obligation to consult would not apply to interference with another state's aggressive use of space. For instance, if a state were using a satellite to corrupt or jam another state's domestic radio waves, that could be seen as an unlawful intervention, justifying immediate, proportional countermeasures necessary to remedy the situation without the necessity for prior consultations. Likewise, proponents of anticipatory self-defense could, on the basis of further intelligence, conclude that the activity was evidence of an imminent armed attack, justifying the use of force. Where the conflict on the definition of "peaceful uses" could become problematic would be if a state decided that, because it viewed all military satellites as non-peaceful, it was free to interfere with them without sanction. This could be used as a purported justification for such actions as the use of blinding lasers against remote sensing satellites.

(5) Concluding Observations on the Outer Space Treaty

In terms of unambiguous limitations on the military uses of outer space, the prohibitions in Article IV stand alone, prohibiting virtually any form of militarization of the moon and celestial bodies, but only the stationing of weapons of mass destruction on orbit, leaving a substantial freedom of action in the formation of national space policy. With this freedom, however, comes the responsibility to use space power in a manner consistent not only with those values underlying the regimes of non-intervention and the use of force, but those specific values of the space-law regime; namely the common interest, non-appropriation and freedom principles.

b) Satellite Broadcasting

Broadcasting by satellite, also knows as direct broadcasting satellites (DBS), direct to home (DTH) or broadcasting satellite service (BSS) involves the beaming of broadcast signals directly from a satellite to end users. In addition to satellite television, which one typically thinks of as occupying this category, new technologies such as portable satellite radio and broadband Internet by satellite are quickly emerging.

One study has concluded the broadband satellite industry could balloon to U.S. $27 Billion by 2008.[297] This expansion is seen by some as the best hope for bridging the "digital divide" between rural and urban areas of the U.S. by providing the former with high speed Internet without the cost of fiber optic cable

---

[297] "Pioneer Consulting Predicts Global Market For Broadband Satellite Services Of $27 Billion By 2008" *Communications Today* 8:12 (17 January 2002).

infrastructure.[298] For the same reasons, the technology could no doubt prove fruitful for developing countries as well. India's Bharti Broadband Networks, Ltd., for instance, is partnering with an Israeli firm to provide high speed Internet access to Indian business and "small office/home office" customers.[299]

Of course, the Internet defies classification as "broadcasting" or telecommunications or really any characterization because the various Internet technologies share traits of all of the communications media. A person can use the Internet to watch a video feed, make a telephone call, send or receive a facsimile or electronic mail message, or even engage an opponent halfway around the world in a virtual aerial dogfight. In many ways, Internet technology is evolving faster than the ability of governments to regulate it. Given the generally reactive nature of international law, it is not surprising that it has little to say on the matter currently. Instead, Internet access is governed in different ways by different national regulatory authorities. Treatments range from the relatively open regimes of the Western Democracies to the extreme case of the Taliban in Afghanistan, which banned all television and Internet access to the populace. At other locations along the continuum are "cyber-dissidents" jailed in China, state-controlled Internet service providers and firewalls put up by governments in Saudi Arabia, and the requirement by the Russian

---

[298] "Satellite Broadband Service Would End Digital Divide, Hughes Executive Tells House Panel" *Satellite News* 24:21 (28 May 2001).

[299] "Bharti Broadband Networks Ltd. Selects Gilat for VSAT Satellite Communications Network" *India Telecom* 13:7 (1 July 2001) 10.

president that Internet service providers channel messages through security forces for potential monitoring."[300]

Turning briefly to the more settled area of DBS, it is important to note that the freedom of information principle, largely dominating the landscape in the area of terrestrial broadcasting, has been beset by international attempts to assure that it does not pertain to satellite broadcasting. The first significant measure along this road was found in the Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting (1982), adopted by General Assembly resolution pursuant to a vote of 107 votes in favor, 13 against and 13 abstentions, with the votes against consisting of Japan, Israel, the U.S. and several Western European nations. The provision directly undermining the concept of freedom of information was found in paragraphs 13 and 14, requiring a state to enter into consultations with other states where an international broadcasting service was contemplated and further requiring that such service only be established on the basis of agreements and/or arrangements with said state.[301] This freedom was further limited by a resolution adopted by the ITU at the 1997 World Radiocommunication Conference, requiring, in addition to technical coordination rules already in place, that administrations obtain agreements from other countries before providing DBS service across national boundaries. Though the resolutions were non-binding, commentators worried because they were given weight by ITU institutions in

---

[300] P. K. Yu, "Symposium: Bridging The Digital Divide: Equality In The Information Age: Forward" (2002) 20 Cardozo Arts & Ent. L. J. 1 at 37.

[301] *Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting*, GA Res. 37/92, UN GAOR, 100th Sess., UN Doc. A/RES/37/92 (1982).

interpreting technical coordination rules.[302] Thus, those states seeking to limit the freedom of broadcasting have largely achieved their objective, not by outlawing it, but by making it administratively impossible. One must recall, however, that per the ITU Constitution, government and military uses are explicitly exempted from all but the harmful interference rules, and even that prohibition only requires avoiding interference as far as possible. Thus, to the extent a military or government satellite is able to broadcast into a particular territory without interfering with existing radio frequency uses, there is no binding authority to prohibit the practice. Of course, the more significant impediment to the current use of satellite broadcast technology for psychological operations purposes is the fact that most intended audiences currently lack the required equipment to receive the signals.

c) Implications for IW

To date, military space assets have largely fulfilled the mission of "information in warfare," acting to enhance the capabilities of air, land and sea weapons and providing a vital role in providing the intelligence and communication necessary for effective command and control. All indications are that the future portends that space will become a medium through which information is used, not to make other weapons more effective, but as a weapon itself. It is difficult to conceive of an IW technique that could be deemed a weapon of mass destruction, thus it is unlikely that IW platforms will fall within a specific treaty prohibition. Nonetheless, decision-makers should be guided by the principles found in the applicable outer

---

[302] G. E. Oberst, Jr., "Satellite Broadcasting Prior Consent" *Via Satellite* 13:2 (1 February 1998).

space law. To the extent IW assets are able to make conflict more precise and/or less deadly, it would seem that their use would serve the common interest principle. An electronic or physical attack, disabling a satellite being used in a hostile manner could be justified in terms of the freedom principle, which does not extend to non-peaceful uses, but by creating a disabled satellite, or worse a huge field of space debris, it could be viewed as a contamination of the outer space environment having a potentially disproportionate impact on the freedom of all states to peacefully use outer space. When and if lasers and other weapons are stationed in outer space, the link between the freedom principle and its corresponding duty of peaceful use will become even more important. Interception and destruction of missiles before they reach the outer space portion of their trajectory would seem in accord with the school of thought equating peaceful uses with non-aggressive uses. The use of a laser against domestic infrastructure in response to a low-level intervention; however, would likely not. While the absence of prohibition leaves a wide area of freedom in the military use of outer space, the internationally recognized goals embodied in the Outer Space Treaty counsel restraint even in excess of that attendant to coercion in the earthly environment.

E. Law of Armed Conflict

Traditionally, two broad bodies of law relating to the subject of armed conflict existed. The *jus ad bellum*, discussed above, governed the legality of resorting to the use of force in the settlement of a dispute, while the *jus in bello* (also referred to as the Law of Armed Conflict or LOAC) described what particular actions are permissible in the prosecution of hostilities. As previously noted, contemporary

practice has increasingly blurred the distinction between wartime and peacetime. In response, the principles regarding the application of the LOAC have generally broadened to assure the widest application of its humanitarian ends.[303] This section will examine the elements of the LOAC, both as a review of the norms that will apply to IW applications in an armed conflict situation, but also to identify principles that should guide the application of IW in low intensity conflicts. This approach is consistent with U.S. Department of Defense policy of applying the LOAC principles across the entire spectrum of conflict.[304]

1. Interaction with General Public International Law

Historically, a state of war between two nations served to negate any treaty obligations between or among the belligerents. Since the adoption of several conventions laying down "rules of warfare" and more recently, the adoption of the U.N. Charter, this generalization has become increasingly limited in its application. Obviously, rules of warfare would have no meaning if the existence of conflict served as an excuse for disregarding them. The overriding contemporary presumption is derived from the concept of "fundamentally changed circumstances" such that it can generally be said that treaties inconsistent with the state of war are considered suspended during such state.[305]

---

[303] See *supra* Section III.C.1.

[304] M.E. Guillory, "Civilianizing the Force: Is the United States Crossing the Rubicon" (2001) 51 A.F. L. Rev. 111 at 113, citing Chairman, Joint Chiefs Of Staff, CJCSI 5810.01a, "Implementation Of The DoD Law Of War Program" (27 August 1999) at 5a.

[305] Detter, *supra* note 123 at 346-349.

The fundamental change principle is codified in Article 62 of the Vienna Convention on the Law of Treaties.[306] A fundamental change of circumstances between the parties may form the basis for terminating, withdrawing from or suspending the operation of a treaty between two parties if certain conditions are met. The presumption is that a fundamental change will not affect the parties' treaty relationship; however, the Vienna Convention does recognize an exception to the general rule where the circumstances changed formed "an essential basis of the consent of the parties to be bound..." and the change radically changes the extent of obligations still to be performed under the treaty.[307]

A 1985 resolution of the *Institut de Droit International*, proposed a meaningful framework for addressing the issue, denominating certain types of treaties that are invariably inconsistent with a state of war and others that generally should enjoy a presumption of continuance. To the former classification belong such instruments as alliances or mutual defense pacts involving both belligerents and conventions relating to the territorial sovereignty of one belligerent to the exclusion of the other. Conspicuous among members of the latter classification are treaties establishing international organizations such as the United Nations, the Universal Postal Union and the ITU.[308] Of particular significance to IW is the fact that the regulations promulgated by such bodies were not identified as enjoying the same presumption. Thus, while these precepts recognize that the existence of a valuable

---

[306] *Convention on the Law of Treaties*, 23 May 1969, 8 I.L.M. 679 [hereinafter Vienna Convention]. Although the United States has not ratified the Vienna Convention, it is, for the most part, regarded as declaratory of customary international law. See introductory note Part III, *Restatement, supra* note 154.

[307] *Ibid.*

[308] Detter, *supra* note 123 at 346-349.

organization such as the ITU should not be jeopardized by a state of war, certain of its rules, such as the rules dealing with harmful interference, are inconsistent with a state of hostility at least as they apply between belligerents.

2. Overriding Principles

Though different commentators emphasize different elements, the LOAC can be said to rest on four pillars. Those overriding concepts are necessity, discrimination, proportionality and humanity.[309] The pillars are important in realizing the two overriding purposes of the various instruments comprising the LOAC, which are the limitation of the methods of warfare, referred to as "Hague law" and the protection of certain classes of individuals (i.e. the sick and wounded, civilians and prisoners of war) referred to as "Geneva law".[310]

a) Necessity

The rule of necessity finds its origin in Hague law. For instance the Hague Conventions of 1899 and 1907 both provide, "The right of belligerents to adopt means of injuring the enemy is not unlimited."[311] While the convention goes on to prohibit certain specific methods of warfare, including poisoning and the killing of surrendering troops, another provision prohibited the use of weapons calculated to

---

[309] See M.N. Schmitt, "Humanitarian Law And The Environment" (2000) 28 Denv. J. Int'l L. & Pol'y 265 at 308-312 [hereinafter Schmitt, "Humanitarian Law"], including the concept of proportionality within the category of discrimination and adding chivalry as an additional precept; R.A. Ramey, "Armed Conflict on the Final Frontier: The Law of War in Space," (2000) 48 A.F. L. Rev. 1 at 34-35; S. Oeter, "Method and Means of Combat" in Fleck, *supra* note 119, 105 at 105-109.

[310] See Schmitt, "Humanitarian Law" *Ibid.* at note 1.

[311] *Convention (II) with Respect to the Laws and Customs of War on Land,* 29 July 1899, 32 U.S. Stat. 1803; *Convention (IV) with Respect to the Laws and Customs of War on Land,* 18 October 1907, 36 U.S. Stat. 2227, available in Schindler, *supra* note 118 at 75, Article 22 [hereinafter Hague (1899) and Hague (1907)].

cause "superfluous injury" in the words of the 1899 treaty or "unnecessary suffering" in the 1907 iteration. The obligation to spare religious, artistic, scientific and cultural buildings and the right to prevent the abuse of the protections of a parlementaire advancing under a white flag were couched in terms of taking "all necessary steps."[312] As Professor Schmitt has noted, "Under current norms, an actor must be able to articulate the imperative military advantage intended to be gained by an attack."[313] Thus conceived, necessity can be viewed as the first hurdle any purported operation should have to clear. The importance of clearing this hurdle cannot be understated, as a "grave breach" subjecting a person to penal sanctions is defined as "killing, torture or inhuman treatment, ... willfully causing great suffering or serious injury to body or health, and extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly.[314]

b) Discrimination

In many senses, discrimination and proportionality can be seen as opposite sides of the same coin. Though the prohibition against indiscriminate warfare can attributed to state practice dating back to the 19th century, the rule did not find full expression in the Hague Conventions, which only prohibited discrete types of indiscriminate violence. It was not until the adoption of Additional Protocol I to the to the 1949 Geneva Conventions that the precept was comprehensively codified.[315]

---

[312] *Ibid.* at Articles 27, 33.
[313] Schmitt, "Humanitarian Law" *supra* note 309 at 1083.
[314] Geneva (I), *supra* note 121 at Article 50.
[315] See Oeter, *supra* note 309 at 113. Note: President Reagan declined to forward Protocol I to the U.S. Senate for advice and consent, citing the Protocol's recognition of wars of national liberation as international and the Protocol's extension of combatant status to certain irregular troops,

The basic rule, requiring that combatants "direct their operations only against military targets" is supplemented a definition of indiscriminate attacks as those a) not directed at a specific military objective, b) employing means incapable of being directed at a specific military objective or c) employing means otherwise incapable of being used in accordance with the Protocol.[316]

c) Proportionality

The rule of proportionality is perhaps best stated in the course of elaborating on what is considered an indiscriminate attack. One example of an indiscriminate attack is one "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[317] As has been seen above in relation to the law of countermeasures and the ILC Draft Rules on state responsibility, the concept of proportionality is not unique to the law of armed conflict, but constitutes an overriding principle of restraint, limiting otherwise lawful responsive action.

d) Humanity

In discussing humanity, Schmitt observed that the concept, traditionally stated in terms of preventing useless or superfluous suffering, is largely subsumed in the

---

opining that these measures could give legitimacy to terrorists. President Reagan expressed his regret that those provisions obscured the positive developments represented in the other provisions of the Protocol. "Message From The President Transmitting Protocol II Additional To The 1949 Geneva Conventions, Relating To The Protection Of Victims Of Noninternational Armed Conflicts" (1987) 26 I.L.M. 561. Nonetheless, many other provisions, including those codifying the discrimination principle, are widely recognized as customary international law.

[316] *Additional Protocol I, supra* note 127.

[317] *Ibid.* at Article 51(5)(b).

other principles. After all, suffering that is useless is unlikely to be characterized as unnecessary or disproportionate. He went on to describe them as acts that civilized people intuitively know to be wrong, or stated another way, "acts that civilized people just don't do."[318]

3. Specific Prohibitions

In addition to the broad concepts discussed above, the conventions underlying the LOAC contain numerous specific prohibitions on the types of weapons that may be used and the ways in which they may be employed. Those of potential relevance to IW will be discussed herein.

a) Environmental Modification Techniques

By way of the 1977 Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques (ENMOD), the environment joined civilians and certain civilian structures as subjects of protection by the LOAC.[319] The convention prohibits military or hostile use of environmental modification techniques "having widespread, longlasting or severe effects as the means of destruction, damage or injury to any other State Party." Environmental modification techniques are defined as those aimed at modifying, "through the deliberate manipulation of natural processes – the dynamics, composition or structure of the Earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer

---

[318] Schmitt, "Humanitarian Law" *supra* note 309 at 1084.

[319] *Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques*, 18 May 1977, 31 U.S.T. 333, availabile in Schindler & Toman, *supra* note 118 at 163.

space." The inclusion of outer space is significant considering the basing of weapons in outer space or the use of weapons against space assets, specifically in considering the potential of the destruction of such a platform to arguably alter the composition of outer space by creating a debris field that could be widespread, long lasting and severe in terms of future access to space.

Additional Protocol I, with 160 state parties (the U.S. not being one) broadens environmental protections in wartime in Article 55, which requires states in warfare to "protect the natural environment against widespread, long-term and severe damage." Article 55 expands on ENMOD's "deliberate manipulation" language, further addressing itself to "means of warfare which are intended or may be expected to cause such damage...."[320] Given the Protocol's widespread adoption and the lack of a U.S. objection to this provision, it is arguable customary international law. Furthermore, with the increase of coalition warfare, it is unlikely that the U.S. will ever fight in a coalition that does not include signatories to the Protocol.

Article 56 of Additional Protocol I, however, protecting "Works and Installations Containing Dangerous Forces" is one that the U.S. does object to as creating a different targeting standard than for other infrastructure elements.[321] While the provision is important in providing heightened protection to dams, dykes and nuclear electrical generating stations, the destruction of which could unleash devastating and indiscriminate forces of destruction, it is not an outright ban, still

---

[320] *Additional Protocol I, supra* note 127 at Article 55.

[321] For a discussion of the U.S. position on Article 56, see Schmitt, "Humanitarian Law" *supra* note 309 at 304-306.

admitting exceptions based on heightened considerations of necessity.[322] Since these facilities are largely computer controlled, an IW attack on them is conceivable. Though the rule of proportionality probably leads to the same answer, this specific prohibition demands heightened attention, especially when acting in concert with coalition partners who are signatories to Additional Protocol I.

b) Blinding Lasers

Given the possible use of lasers in fulfillment of the physical attack element of IW, brief discussion is appropriate regarding the Protocol on Blinding Laser Weapons to the 1980 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects.[323] The Protocol is remarkable, not so much for what it prohibits but for what it allows. The scope of prohibition is narrowly addressed only to "laser weapons specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness to unenhanced vision."[324] The Protocol continues to exclude from its coverage, "Blinding as an incidental or collateral effect of the legitimate military employment of laser systems, including laser systems used against optical equipment."[325] The protocol prompts two observations. First, it is clear that the development of laser weapons, especially those

---

[322] *Ibid.*

[323] *Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention)*, 13 October 1995, 105 S. Treaty Doc. 1, online: International Committee of the Red Cress Web Site <http://www.icrc.org/ihl.nsf/> (date accessed: 30 June 2002) [hereinafter *Blinding Laser Protocol*]. The protocol currently has 63 Parties. It was transmitted to the U.S. Senate for advice and consent by President Clinton on 7 January 1997. U.S. Senate Treaty Doc. 105-1 (7 January 1997).

[324] *Blinding Laser Protocol*, *Ibid.* at Article 1.

[325] *Idib.* at Article 3.

that might be used against information infrastructure, is not significantly inhibited by the Protocol. The second observation, made by Schmitt, is that this represents an area where the rule of humanity may run counter to the rule of proportionality in that more lethal means may be required to achieve a valid objection simply because of the antithetical nature of intentional blinding.[326]

c) Perfidy

A potential problem presented by any attempt to subject warfare to rules is the possibility that one party will attempt to use those rules to strategic advantage. The prohibitions against treachery and perfidy[327] have historically prohibited such abuse of the protections of the law of war. The Hague Conventions prohibited a combatant to "kill or wound treacherously individuals belonging to the hostile nation or army."[328] The prohibition as amplified and defined in terms of perfidy in Additional Protocol I is widely recognized as representing customary international law.[329] Article 37 of the Protocol provides, "It is prohibited to kill, injure or capture an adversary by resort to perfidy." Perfidy is then defined as, "Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence...."[330] Thus, such acts as feigning surrender, pretending to be wounded or a civilian, wearing of enemy or neutral state uniforms,

---

[326] Schmitt, "Humanitarian Law," supra note 309 at 309.

[327] Though these terms have different shades of meaning, their meanings overlap so substantially, as do the examples of each in the literature and the consequences flowing from their employment, that they will be discussed under the single term of perfidy for present purposes.

[328] Hague (1899) and Hague (1907), *supra* note 311, Article 23(b).

[329] Detter, *supra* note 123 at 303

[330] *Additional Protocol I*, *supra* note 127 at Article 37.

misuse of the red cross or red crescent as well as the shielding of military troops or objects by such protected facilities as hospitals are all condemned as acts of perfidy.[331] Significantly, one should note that Additional Protocol I only addresses itself to killing, injuring or capturing an adversary, leaving apparently unaffected the right to the use of perfidy to disable facilities or conduct other operations not involving death, injury or capture of persons.[332]

The difficulty of perfidy is not so much in defining it as it is in distinguishing it from "lawful ruses or war" which have historically been an essential element of warfare and have always been recognized as the legitimate counterpart of perfidy. In fact, the same article prohibiting perfidy describes lawful ruses of war as those acts of deception that "do not invite the confidence of an adversary with respect to protection under [international] law."[333] Lawful ruses include the use of camouflage, feigning retreat, communication jamming, transmitting misleading messages, inserting incorrect information into adversary command structures and ambush operations.[334] Thus, the placement by NATO forces of incorrect information into Yugoslav computer defenses was clearly a lawful exercise of IW to conduct military deception. The sending of an electronic communiqué regarding terms of surrender containing a computer virus or a Trojan horse[335] that would damage a system or, unknown to the host, transmit information such as passwords typed back to the sender, would likely

---

[331] See *Idib.* at Articles 37-39; Detter, *supra* note 123 at 303-307; Oeter, *supra* note 309 at 199-203.

[332] Oeter, *supra* note 309 at 201.

[333] *Additional Protocol I, supra* note 127 at Article 37.

[334] Detter, *supra* note 123 at 303-307; Oeter, *supra* note 309 at 199-203.

[335] "Trojan Horses are impostors--files that claim to be something desirable but, in fact, are malicious. Trojans contain malicious code, that, when triggered, cause loss, or even theft, of data." Symantec Knowledge Base, online <http://service2.symantec.com/SUPPORT/ent-security.nsf/pfdocs/1999041209131148> (date accessed: 30 June 2002).

constitute an act of perfidy. If the type of damage done could be expected to kill or injure, it would be an unlawful act of perfidy.

One area where the law of perfidy should raise particular concern with regard to IW involves the interconnected nature of the information infrastructure. For instance, while there is a general obligation not to attack hospitals, many current IW methods lack the discrimination to predictably shut down military objectives without potentially compromising hospitals or emergency response networks. Since the protection afforded hospitals is tied to an obligation not to co-locate them with military targets[336], short of creating separately contained medical and emergency response data networks, mere physical separation could be insufficient to achieve this separation in the cyber realm. To the extent this discrimination is infeasible and the tenets of necessity and proportionality still weigh in favor of information attack, one further obligation obtains to warn the civilian population to the extent circumstances permit so that effective precautions can be taken.[337]

d) Protected Individuals and Objects

The rules of necessity, discrimination and proportionality all involve a juxtaposition of lawful military objectives, on the one hand, with protected individuals and objects on the other. That being the case, it is important to understand what qualifies a potential target as a military objective. Once again, it is Additional Protocol I, that provides the articulation of the standard: "[M]ilitary objectives are limited to those objects which by their nature, location, purpose or use

---

[336] Oeter, *supra* note 309 at 198.

[337] *Ibid.* at 165, citing *Additional Protocol I*, *supra* note 127 at Article 51 and Hague (1899) and Hague (1907), *supra* note 311, Article 57.

make an effective contribution to the military action and whose total or partial destruction, capture or neutralization in the circumstances ruling at the time, offers a definite military advantage."[338] Telecommunications have traditionally been universally accepted as a valid target and technology will only make this more true. As Oeter noted, "The practice of the Kuwait 'Desert Storm' operation in 1991 demonstrated that an attacker nowadays must probably destroy a network of telecommunication *in toto* (or at least its central connection points) in order to paralyze the command and control structures of the enemy armed force, which in themselves clearly constitute a legitimate military objective."[339]

4. The Question of Civilian/Contractor Involvement

One aspect of the increasing importance of technology to the way war is waged is an increasing reliance by military departments on civilian employees and contractors for support and sometimes even operation of elements of war-fighting machinery. While the topic has been treated in depth elsewhere, it is appropriate here to focus briefly on the particular problems posed by the use of civilians in IW operations.[340] The important points to note with regard to civilian involvement is that civilians who participate directly in hostilities are considered unlawful combatants, subject to criminal prosecution.[341] By virtue of their direct contribution to the war effort (as opposed to their civilian status), they would have to be likewise understood to be lawful targets. The difficulty becomes once again one of drawing the line

---

[338] *Additional Protocol I*, *supra* note 127 at Article 52.
[339] Oeter, *supra* note 309 at 161.
[340] For an excellent, in-depth discussion of the topic, see Guillory, *supra* note 304.
[341] *Ibid.* at 115.

between direct and indirect participation. Manufacturing has generally not been considered direct participation so that munitions manufacturers (though they and their plants may be military objectives) are not considered subject to prosecution as unlawful combatants.[342] At some point, however, a computer programmer who writes the code necessary to find and compromise an enemy system starts to look more like a weapon loader or aimer than a manufacturer.[343] Is it possible that the determination of combatant status could turn on the nuances of computer programming code, which in the ultimate sense is just a differing configuration of 1's and 0's? Will a programmer who writes a self-executing program, launchable at the touch of a button, be a combatant, subject to criminal prosecution if he falls into the hands of the enemy or even to prosecution as a war criminal[344], while the person in the next cubicle, who wrote a program requiring a military technician to enter extensive parameters in order to acquire a target would be a mere manufacturer? These lines are not clearly drawn, counseling extreme caution in assigning civilians to offensive information operations positions and in devising contract specifications for offensive information operations capabilities.[345]

F. IW, Intervention and Community Values

Having scanned the repertoire of international law, several resonant themes have emerged, some combining from multiple sources and others sounding in

---

[342] *Ibid.* at 134.
[343] *Ibid.* at 128.
[344] *Ibid.* at footnote 32.
[345] *Ibid.* at 136, noting that even defensive information operations could be problematic if they could possibly cause damage to the enemy. This observation is particularly prescient given the potential development of "active defense" techniques mentioned *supra*.

isolation. The players have included the various international treaties and customary precepts underlying the *jus ad bellum* as well as the principle of non-intervention and the *jus in bello*. The emergence of international law to deal with the contemporary threats of cybercrime and cyber-terrorism has contributed, as have the elements of international telecommunication law that govern the media which may serve as a pathway for information attacks. The diversity of sources, as well as the diversity of academic views have sometimes revealed areas of harmony, clearly identifying agreed norms, but have often uncovered discord with little prospect for resolution, at least in the short term. It is now appropriate, in conclusion, to review those areas of assonance to be considered solid bases for future reliance and those of dissonance that should inform further inquiry and guide the making of the most difficult decisions.

The Charter of the United Nations and its regime relevant to the use of force, though some would argue that it is imperiled by overly restrictive interpretation, recognizes universally accepted values of sovereignty, territorial integrity, political independence, self-protection and the peaceful resolution of disputes. It's preference for collective security, though largely unrealized during the Cold War, provides the hope for unity in pursuing other values implicit in the charter such as human rights. The value of sovereignty has found further iteration in the non-intervention principle, which, despite controversy as to its scope, is the basis for respecting self-determination and self-governance. International human rights law also contributes widely held values about human dignity and freedom. Though some views of sovereignty and non-intervention would render these human rights illusory for many,

a more flexible approach to international law finds it capable of responding to human suffering and oppression while still respecting the exercise of "rightful sovereignty."

Perhaps no area of this inquiry has been of more contemporary significance than the renewed determination since September 11, 2001, by the international community to uphold the values undermined by international terrorism. Though traditionally an area of international law stunted by political differences, images of indiscriminate suffering and destruction have led to a greater international realization across the whole of international relationships of the timeless virtue enshrined in the law of armed conflict of civilian inviolability. It can hardly be argued that any political agenda, in time of war or peace is sufficient justification for striking at civilians for no other reason than inciting fear and terror.

The law emerging to combat the threats posed by those willing to abuse and exploit new technologies has likewise contributed to the discussion of contemporary international values. Data Integrity, system integrity and privacy of communications, though perhaps not enjoying a universally recognized pedigree, are increasingly being recognized as indispensable for the continued security and growth of the information economy and the promise many feel it holds for worldwide progress.

International communications is an integral part of several ongoing geo-political trends. Regardless of one's views of the desirability of such forces as globalization or privatization, they are shaping the future and they are fueled by an increasingly robust global information infrastructure. That infrastructure depends on values like non-interference in order to realize other values like universal service and public safety as well as long recognized human rights such as the freedom to impart

and receive information. While the law of outer space has enforced principles such as non-interference, it has also seen developments limiting freedom of information. Widespread agreement that outer space should be used peacefully is undermined by fundamental disagreements as to what the term means, reflecting a far more fundamental conflict as to whether peace is better achieved through strength or disarmament. Nonetheless, the obligation to use outer space responsibly should be underscored by the realization that outer space does not rehabilitate and recycle itself and thus is not as resilient as the terrestrial environment.

Finally, the cornerstone concepts of the law of armed conflict; necessity, proportionality, discrimination and humanity, not only encapsulate the limitations on the application of force, but in reality provide a model of restraint suitable for the whole of international relations. They give meaning to the codification at The Hague in 1899 of the concept that the means and methods of warfare are not unlimited, or to put it in the words of that fundamental tenet of civilized society, "the ends do not justify the means."

Having identified several values, all of at least some degree of international normative probity, it is appropriate to overlay them across the analytical framework of the various forms of IW. Thus, this thesis will conclude by returning to those applications of IW identified in Part II and identifying those values most suited to guide decision-makers in their implementation.

1. Psychological Operations

Psychological operations involve the transmission of information, perhaps accurate, perhaps not, to a target audience for the purpose of influencing them. The

values underlying the concept of freedom of information are particularly relevant, as those values have traditionally taken precedence over sovereignty concerns in international law and in international relations. Though this precedence is arguably reversed (at least in a *de facto* sense), in the case of outer space, that may not be the case with regard to military satellites, not subject to the technical requirements of the ITU. This freedom of information is limited, however, by a responsibility reminiscent of the non-intervention principle, not to use it to instigate revolt or armed violence. As a final note, though the freedom of information principle does not necessarily prohibit transmitting false information, purposefully doing so, especially in peacetime, impacts the value of data integrity to some degree and would hopefully be curtailed by political considerations nonetheless.

2. Electronic Warfare

Certainly, none of the values identified is more relevant to electronic warfare than the principle of non-interference. With the close relationship between interference-free communications and public safety, particularly in terms of emergency response and the importance of GPS for navigation as well as search and rescue, electronic warfare techniques, especially in operations short of war, are likely, short of applying physical force, most likely to be viewed as an unlawful intervention or even as a use of force. For that reason, close attention must be paid to the circumstances purportedly justifying an application of electronic warfare and to whether the planned technique can be accomplished with sufficient discrimination to meet the requirement of proportionality.

3. Military Deception

Military deception, at least in the IW context, impacts the emerging values embodied in the Cybercrime Convention of data integrity and system integrity. In the prosecution of armed hostilities, deception is only limited by the prohibition against perfidy, while with operations short of war considerations of the effect of the deception should be weighed against the values of data and system integrity and likely against the backdrop of the particular political situation at the time. For instance, in response to a low-level intervention by one state, another could respond with a deceptive operation designed to give the false impression that a military response was imminent. While this might be less likely to be viewed as a prohibited threat or use of force, a proponent of anticipatory self-defense could hardly be heard to object if it were so perceived and as such formed the basis for a forceful preemptive strike.

4. Physical Attack

Physical attack is probably the easiest of the IW scenarios to deal with, as the regime underlying the physical application of force has certainly had the benefit of decades of development. While it is true that these developments are somewhat obscured, at least regarding the question of humanitarian intervention, there remains widespread agreement that an armed attack justifies an armed response, while a threat or breach of the peace can be sufficient to justify an armed response at the direction or with the permission of the Security Counsel. Thus, though there is disagreement at the periphery, and unfortunately the trend may be for that periphery to become more

central, the U.N. system is still the primary means for defining the proper interaction between the values of sovereignty and self-preservation.

5. Information Attack

If physical attack is the easiest, information attack is probably the most difficult of the IW applications to evaluate. This is, in part, because the details of how this mission is likely to be carried out are largely subject to guesswork and speculation. An information attack against dykes, dams or nuclear plants could certainly impact values such as public safety, discrimination and proportionality while a "denial of service" attack aimed a crippling an e-mail system or an air base computer network would be more difficult to tie to such vital interests. It is far from clear whether the regime related to the use of force will be expanded to apply to information attacks or even whether it should except in the case of those causing damage indistinguishable from an armed attack. In time of conflict, information attack should not be evaluated any differently than any other attack. The time-tested rules of the LOAC are sufficient for that purpose. Though IW technologies, their ability to be implemented from a distance and the use of civilians in their development and employment create difficult issues, the basic task remains one of achieving legitimate and necessary ends by the most discriminate, proportionate and humane means possible. Short of armed conflict, the values underlying the non-intervention principle should provide a sufficient guide. In considering an information attack one should consider what international obligation the other party has violated, the effect the operation will have on the legitimate exercise by that state

of its sovereignty and whether that effect is proportionate to the end of remedying the violation, taking into account the feasibility of less coercive means.

6. Defensive IW

Defensive IW has largely been considered a law enforcement activity and will likely remain so. Nonetheless, as cyber-criminals move from pursuing goals of mischief and personal financial gain and begin to take on the political agendas and the destructive tendencies of terrorists, engaging in ever more damaging attacks and hiding behind the sovereignty of states complicit in their acts through outright support or failure to exercise control, the value of national security will, at some point, have to take precedence over those values favoring a law enforcement response. The issue of "active defense" should be approached with a special degree of caution, especially if it presents the possibility of involving civilians in the application of military power. To the extent active defense is limited to tracking and identifying intruders, it is probably not problematic from an international standpoint, but applications beyond that could be.

V. Conclusion

Information Warfare, like the revolutionary military developments that have preceded it, represents elements of hope and of trepidation. Used responsibly, it represents the hope of resolving disputes that would previously have been resolved with guns and bombs with electrons instead. Furthermore, it provides the next logical step toward the hope realized in large measure in Operation Desert Storm of using technology to reduce the duration and the devastation of armed conflict, particularly

as to civilian populations. With these opportunities come corresponding risks in the form of opportunities for those whose use of these technologies would be less scrupulous. There can no longer be doubt that there are those desirous of the ability and possessed of the inclination to use any available means to bring about the ruin of those values held by the community of civilized nations. This reality will require the wise discernment of visionary leaders and innovative thinkers in the fields of technology, politics, military affairs and of law, to name only a few. Those values that have found collective expression in the treaties and customs that make up the international law, while they cannot substitute for this discernment, can and should form the foundation of the wisdom that underlies it. Those values identified herein, it is hoped, will be of assistance to this undertaking.

Bibliography

Treaties

"Agreed Statements Annexed to SALT II Treaty" 18 I.L.M. 1112 (1979).

Agreement On Telecommunications Services (Fourth Protocol To General Agreement On Trade In Services), March 1997, 36 I.L.M. 354.

Comprehensive Test Ban Treaty, 35 I.L.M. 1439 (1996).

Constitution of the International Telecommunications Union, Dec. 22, 1992, S. Treaty Doc. No. 104-34 (1996) (as amended through 1994).

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949; 75 U.N.T.S. 31.

Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949, 75 U.N.T.S. 85.

Convention (III) Relative to the Treatment of Prisoners of War, 12 August 1949; 75 U.N.T.S. 135.

Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 75 U.N.T.S. 287.

Convention (II) With Respect to the Laws and Customs of War on Land, 29 July 1899, 32 U.S. Stat. 1803.

Convention (IV) with Respect to the Laws and Customs of War on Land, 18 October 1907, 36 U.S. Stat. 2227.

Convention for the Protection of Submarine Cables, 14 March 1884, 24 Stat 989.

Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 23 September 1971, 24 U.S.T. 565.

Convention for the Suppression of Unlawful Seizure of Aircraft, 16 December 1970, 22 U.S.T. 1641.

Convention on Cybercrime, 23 Novemer 2001, Eur. T.S. no 185, 41 I.L.M. 282.

Convention on International Civil Aviation, 7 December 1944, 15 U.N.T.S. 295.

Convention on Offences and Certain Other Acts Committed on Board Aircraft, 14 September 1963, 20 U.S.T. 2941.

Convention on the Continental Shelf, 29 April 1958, 15 U.S.T. 471.

Convention on the High Seas, 29 April 1958, 13 U.S.T. 2312.

Convention on the Law of Treaties, 23 May 1969, 8 I.L.M. 679.

Convention on the Marking of Plastic Explosives for the Purpose of Detection, 1 March 1991, 30 I.L.M. 721.

Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques, 18 May 1977, 31 U.S.T. 333.

Convention (III) Relative to the Opening of Hostilities, 18 October 1907, 36 U.S. Stat. 2259.

International Convention for the Suppression of the Financing of Terrorism, 9 December 1999, 39 I.L.M. 270.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 16 I.L.M. 1391.

Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention), 13 October 1995, 105 S. Treaty Doc. 1.

Protocol Relating to an Amendment to the Convention on International Civil Aviation, 10 May 1984, 23 I.L.M. 705.

Statute of the International Court of Justice, 26 June 1945, 59 Stat. 1031.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 January 1967, 610 U.N.T.S. 205.

Treaty on the Limitation of ABM Systems and Interim Agreement and Protocol on the Limitation of Strategic Offensive Arms, 11 I.L.M. 784 (1972).

Treaty On Underground Nuclear Explosions For Peaceful Purposes, 15 I.L.M. 891 (1976).

United Nations Convention on the Law of the Sea, 10 December 1982, 1833 U.N.T.S. 3.

International Resolutions

Declaration on Measures to Eliminate International Terrorism, GA Res. 60, UN GAOR, 49th Sess., Supp. No. 49, U.N. Doc. A/49/743 (1994) at 303.

Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States, G.A. Res. 2526(XXV), U.N. GAOR, 25th Sess., Supp. No. 28, UN Doc. A/8028 (1970).

Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism, G.A. Res. 210, U.N. GAOR, 51st Sess., Supp. No. 49, at 346, U.N. Doc. A/51/631 (1996).

Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, GA Res. 37/92, UN GAOR, 100th Sess., UN Doc. A/RES/37/92 (1982).

Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83 UN GAOR, 53rd Sess., UN Doc. A/56/PV.85 (2002).

Jurisprudence

Asylum Case(Columbia v. Peru), [1950] I.C.J. Rep. 266.

Case Concerning Military And Paramilitary Activities In And Against Nicaragua (Nicaragua v. United States of America)(Merits), [1986] I.C.J. Rep. 14.

The Corfu Channel Case (Merits), [1949] I.C.J. Rep. 4.

North Sea Continental Shelf Case, [1969] I.C.J. Rep. 3.

Steamship Lotus Case (France v. Turkey) (1927), P.C.I.J. (Ser. A) No. 10.

Legislation and Regulations

10 U.S.C. §§ 371-382.

18 U.S.C. § 1385.

18 U.S.C. §§ 2331-2339B.

22 U.S.C. §§ 2651–2728.

22 C.F.R. § 121.

47 U.S.C. § 606.

47 U.S.C. § 606.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub.L. No. 107-56, 115 Stat. 272.

Books and Treatises

Brownlie, I. *International Law and the Use of Force By States*, (London: Oxford University Press, 1963).

Brownlie, I. *Principles of Public International Law*, (5th ed.) (Oxford: Clarendon Press, 1998).

Cybercrime... Cyberterrorism... Cyberwarfare...: Averting an Electronic Waterloo, (Washington, D.C.: Center for Strategic and International Studies, 1998).

Detter, I. *The Law of War*, 2nd ed. (Cambridge: Cambridge University Press, 2000).

Dinstein, Y. *War, Aggression and Self-Defense*, 3rd ed. (Cambridge: Cambridge University Press, 2001).

Erickson, R. *Legitimate Use of Military Force Against State-Sponsored International Terrorism*, (Maxwell AFB AL: Air University Press, 1989).

Fleck, D. ed., *The Handbook of Humanitarian Law in Armed Conflicts* (Oxford: Oxford University Press, 1999).

Glennon, M. *Limits of Law, Prerogaties of Power: Intervenionism After Kosovo* (New York: Palgrave, 2001).

Gongora, T. & von Riekhoff, H. eds., *Toward a Revolution in Military Affairs? Defense and Security at the Dawn of the Twenty-First Century*, (Westport Conn.; London: Greenwood Press, 2000).

Gray, C. *International Law and the Use of Force*, (New York: Oxford University Press, 2000).

Matte, N.M., *Aerospace Law: Telecommunications Satellites*, (Toronto: Butterworths, 1982) at 68.

McDougal, M.S. & Feliciano, F.P. *Law and Minimum World Public Order: The Legal Regulation of International Coercion* (New Haven: Yale University Press, 1961).

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

Schindler, D. & Toman, J. eds., *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions and Other Documents* (Dordrecht, Netherlands: Marinus Hijhoff Publishers, 1988).

Schwartzstein, S.J., ed., *The Information Revolution and National Security, Dimensions and Directions* (Washington D.C.: Center for Strategic and International Studies, 1996).

Sharp, W.G., Sr., *Cyberspace and the Use of Force*, (Falls Church VA: Aegis Research Corp., 1999).

Simma, B., Ed., *The Charter of the United Nations: A Commentary* (Oxford: Oxford University Press, 1994).

Slaughter, A. & Burke-White, W. "Focus: September 11, 2001--Legal Response to Terror: An International Constitutional Moment" (2002) 43 Harv. Int'l L.J. 1.

Teson, F.R. *Humanitarian Intervention: An Inquiry Into Law and Morality* 2nd ed., (Irvington-on-Hudson, NY: Transnational Publishers, Inc., 1997).

Official Government Publications

Ballistic Missile Defense Agency, "Fact Sheet: Space Based Laser (SBL)" (2002), online: Ballistic Missile Defense Agency Web Site <http://www.acq.osd.mil/bmdo/bmdolink/pdf/sbl.pdf> (date accessed: 3 July 2002).

Chairman, Joint Chiefs Of Staff, CJCSI 5810.01a, "Implementation Of The DoD Law Of War Program" (27 August 1999).

Joint Chiefs of Staff, Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms" (12 April 2001).

Joint Chiefs of Staff, Joint Publication 3-07, "Joint Doctrine for Military Operations Other Than War" (16 June 1995); Secretary of the Air Force, Air Force Doctrine Document 1, "Air Force Basic Doctrine" (1 September 1997).

Joint Chiefs of Staff, Joint Publication 3-13, "Joint Doctrine for Information Operations" (9 October 1998).

Joint Chiefs of Staff, Joint Publication 3-58, "Joint Doctrine for Military Deception" (31 May 1996).

Office of the President of the United States, Press Release "President Discusses National Missile Defense" (13 December 2001), online: White House Web Site <http://www.whitehouse.gov/news/releases/2001/12/20011213-4.html> (date accessed: 3 July 2002).

Office of the President of the United States, "Remarks of the President at 2002 Graduation Exercise of the United States Military Academy" 1 June 2002.

"Message From The President Transmitting Protocol II Additional To The 1949 Geneva Conventions, Relating To The Protection Of Victims Of Noninternational Armed Conflicts" (1987) 26 I.L.M. 561.

President of the United States, Presidential Decision Directive NSTC-6, (online: http://www.spacecom.af.mil/usspace/gps_support/documents/gps_pdd.htm).

U.S. Department of the Air Force, Air Force Doctrine Document 1, "Air Force Basic Doctrine" (September 1997).

U.S. Department of the Air Force, Air Force Doctrine Document 2-5 "Information Operations" (5 August 1998).

U.S. Department of the Air Force, Air Force Doctrine Document 2-5.1, "Electronic Warfare" (19 November 1991).

U.S. Department of the Navy, MCWP 3-40.4, "Information Operations" (coordinating draft, 10 December 2001).

U.S. Department of the Navy, "Navy Information Warfare Strategic Plan: IW—Capabilities for the New Millenium" (undated).

U.S. Department of State, "United States Statement, 55 UNGA Sixth Committee, Agenda Item 159, Report of the International Law Commission" October 27, 2000.

U.S. Space Command, "United States Space Command Vision for 2020" February 1997, online <http://afpubs.hq.af.mil>.

Articles

Baker, S. "Comparing the 1993 U.S. Airstrike on Iraq to the 1986 Bombing of Libya: The New Interpretation of Article 51" (1994) 24 Ga. J. Int'l & Comp. L. 99.

"Bharti Broadband Networks Ltd. Selects Gilat for VSAT Satellite Communications Network" *India Telecom* 13:7 (1 July 2001) 10.

Bond, L. "The GNSS Safety and Sovereignty Convention of 2000 AD" (2000) 65 J. Air L. & Com. 445.

D'Amato, A. "Trashing Customary International Law" (1987) 81 A.J.I.L. 101.

"EW Expands Into Information Warfare" *Aviation Week & Space Technology*, 141:15 (10 October 1994) 47.

Franck, T.N. "Appraisals Of The ICJ's Decision: Nicaragua V. United States (Merits)" (1987) 81 A.J.I.L. 116.

Freedman, D. "Information Warfare" *Technology Review* 104:9 (1 November 2001) 61.

Fulghum, D. "Cyber-Arsenal Needs Testing" *Aviation Week and Space Technology* 154:9 (26 February 2001) 57.

Fulghum, D.A. "Pentagon Reveals Mobile Pain Ray" *Aviation Week & Space Technology* 154:19 (7 May 2001) 82.

Fulghum, D.A. & Wall, R. "Combat-Proven Infowar Remains Underfunded" *Aviation Week & Space Technology* 154:9 (26 February 2001) 52.

Fulghum, D.A. & Wall, R. "Information Warfare Isn't What You Think" *Aviaiton Week & Space Technology* 154:9 (26 February 2001) 52.

Fulghum, D.A. & Wall, R. "New Tools Emerge For InfoWar Battle" *Aviation Week & Space Technology* 154:9 (26 February 2001) 58.

Fulghum, D.A. & Wall, R. "U.S. Shifts Cyberwar To Combat Commands Intelligence-Gathering, Electronic Attack and Information Manipulation are at Last Being Integrated for Combat" *Aviation Week & Space Technology* 154:9 (26 February 2001) 50.

Guillory, M.E. "Civilianizing the Force: Is the United States Crossing the Rubicon" (2001) 51 A.F. L. Rev. 111.

Jakhu, R. and Rodriguez Serrano, V., "International Regulation of Radio Frequencies for Space Services" Project 2001, Group on Telecommunications (2000).

Kotaite, A. "ICAO's Role With Respect to the Institutional Arrangements and Legal Framework of Global Navigation Satellite System (GNSS) Planning and Implementation" (1996) 21 Ann. Air & Sp. L. 195.

Morison, F.L. "Appraisals Of The ICJ's Decision: Nicaragua V. United States (Merits)" (1987) 81 A.J.I.L. 160.

Murphy, S. "Terrorism And The Concept Of 'Armed Attack' In Article 51 Of The U.N. Charter" (2002) 43 Harv. Int'l L.J. 41 at 48.

Oberst, Jr., G.E., "Satellite Broadcasting Prior Consent" *Via Satellite* 13:2 (1 February 1998).

"Principles Of International Law Concerning Friendly Relations And Co Operation Among States" in *Yearbook of the United Nations* (New York: United Nations, 1970).

"Pioneer Consulting Predicts Global Market For Broadband Satellite Services Of $27 Billion By 2008" *Communications Today* 8:12 (17 January 2002).

Ramey, R.A. "Armed Conflict on the Final Frontier: The Law of War in Space," (2000) 48 A.F. L. Rev. 1.

Reisman, W.M. "Symposium: Legal Responses to International Terrorism" (1999) 22 Hous. J. Int'l L. 3 at 60.

Satellite Broadband Service Would End Digital Divide, Hughes Executive Tells House Panel" *Satellite News* 24:21 (28 May 2001).

Schachter, O. "United Nations Law" (1994) 88 A.J.I.L. 1.

Schmitt, M.N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" (1999) 37 Colum. J. Transant'l L. 885.

Schmitt, M.N. "Humanitarian Law And The Environment" (2000) 28 Denv. J. Int'l L. & Pol'y 265.

Sofaer, A. "International Law and Kosovo" (2000) 36 Stan. J Int'l L. 1 at15.

Stefik, M. & Silverman, A. "The Bit and the Pendulum: Balancing the Interests of Stakeholders in Digital Publishing" (1999) 16 The Computer Lawyer 1.

Strobel; W.P. "A Glimpse of Cyberwarfare" *U.S. News & World Report* 128:10 (13 March 2000) 32 at 32.

Teson, F.R. "Appraisals Of The ICJ's Decision: Nicaragua V. United States (Merits)" (1987) 81 A.J.I.L. 173.

Thomas, T. "China's Electronic Strategies" *Military Review* 81:3 (1 May 2001) 47.

Tiboni, F. & Robb, K. "Agencies Prepare To Hit Back At Hackers" *Federal Times* 37:42 (19 November 2001) 1.

Vlasic, I.A. "Some Thoughts on Negotiating and Drafting Arms Control and Disarmament Agreements Relating to Outer Space" in N.M. Matte, ed., *Arms Control and Disarmament In Outer Space: Towards A New Order Of Survival* (Montreal, Canada: Cener for Research in Air and Space Law, McGill University, 1991) 203.

I.A. Vlasic, "Space Law and the Military Applications of Space Technology," in N. Jasentuliyana, ed., *Perspectives on International Law* (Boston: Kluwer Law International, 1995).

Wall, R. "USAF Defining New Special Mission Aircraft " *Aviation Week & Space Technology* 154:23 (4 June 2001) 32.

Wall, R. "F-14s Add Missions In Anti-Taliban Effort" *Aviation Week & Space Technology* 155:21 (19 November 2001) 38.

White, H.M. Jr. & Lauria, R. "The Impact of New Communication Technologies on International Telecommunication Law and Policy: Cyberspace and the Restructuring of the International Telecommunication Union" (1995) 32 Cal. W. L. Rev. 1.

Wilson, J.R. "The Terrorism Threat, Information Warfare Aims Revolve Around Countering" *Military & Aerospace Electronics* 12:10 (October 2001) 14.

Wright, R.H. "Information Operations: Doctrine, Tactics, Techniques And Procedures" 81:2 (1 March 2001) Military Review 30.

Yu, P.K. "Symposium: Bridging The Digital Divide: Equality In The Information Age: Forward" (2002) 20 Cardozo Arts & Ent. L. J. 1.

Newspaper Stories

Becker, E. "Computer Hackers Are Stopped; Pentagon Networks Were Victim" *The New York Times [Late Edition]* (5 March 1999) A16.

Becker, E. "Pentagon Sets up New Center for Waging Cyberwarfare" *The New York Times [Late Edition]* (8 October 1999) A16.

Editorial, "Striking First," *The New York Times* (23 June 2002) D12.

Gellman, B. "Cyber-Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say" *The Washington Post [Final Edition]* (27 June 27 2002) A1.

Janofsky, M. "New Security Fears As Hackers Disrupt 2 Federal Web Sites" *The New York Times [Late Edition]* (29 May 1999) A1.

"Pentagon Acknowledges Hacker Intrusion Into a Computer System" *The New York Times [Late Edition]* (22 April 1998) A16.

Rubin, J.P. "Countdown to a Very Personal War" *The Financial Times* (30 September 2000) 9.

Sanger, D.E. "Bush to Formalize a Defense Policy of Hitting First" *The New York Times [Late Edition]* (17 June 2002) A1.