COMPUTER NETWORK ATTACK AND THE USE OF FORCE IN INTERNATIONAL LAW: THOUGHTS ON A NORMATIVE FRAMEWORK

MICHAEL N. SCHMITT

June 1999

Research Publication 1
Information Series

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 1999		**00-00-1999 to 00-00-1999**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **HQ USAFA/DFPS,Institute for Information Technology Applications,2354 Fairchild Drive Suite 6L16D,USAF Academy,CO,80840-6258**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This Article explores the acceptability under the jus ad bellum, that body of international law governing the resort to force as an instrument of national policy of computer network attack. Analysis centers on the United Nations Charter?s prohibition of the use of force in Article 2(4), its Chapter VII security scheme, and the inherent right to self-defense codified in Article 51. Concluding that traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by CNA, the Article proposes an alternative normative framework based on scrutiny of the consequences caused by such operations.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**41**	

ABOUT THE AUTHOR

Michael N. Schmitt is Professor of International law, George C. Marshall European Center for Security Studies. A retired Air Force Judge Advocate, he has previously served on the faculties of the United States Air Force Academy and Naval War College, and has been a Visiting Scholar at Yale Law School. While on active duty, Professor Schmitt held a variety of operational assignments including Staff Judge Advocate for Operations, NORTHERN WATCH and PROVIDE COMFORT (air component). He is editor of the Law of Military Operations, Levie on the Law of War and The Law of War: Into the Next Millennium, and has authored many articles, within the United States and abroad, on international law and military operations.

This article also appears in The Columbia Journal of Transnational Law, Volume 37, 1999, pages 885-937.

About the Institute

The Institute for Information Technology Applications (IITA) was formed in 1998 to provide a means to research and investigate new applications of information technology. The Institute encourages research in education and applications of the technology to Air Force problems that have a policy, management, or military importance. Research grants enhance professional development of researchers by providing opportunities to work on actual problems and to develop a professional network.

Sponsorship for the Institute is provided by the Secretary of the Air Force for Acquisition, the Air Force Office of Scientific Research, and the Dean of Faculty at the U.S. Air Force Academy. IITA coordinates a multidisciplinary approach to research that incorporates a wide variety of skills with cost-effective methods to achieve significant results. Proposals from the military and academic communities may be submitted at any time since awards are made on a rolling basis. Researchers have access to a highly flexible laboratory with broad bandwidth and diverse computing platforms.

To explore multifaceted topics, the Institute hosts single-theme conferences to encourage debate and discussion on issues facing the academic and military components of the nation. More narrowly focused workshops encourage policy discussion and potential solutions. IITA distributes conference proceedings and other publications nation-wide to those interested or affected by the subject matter.

ABSTRACT

This Article explores the acceptability under the jus ad bellum*, that body of international law governing the resort to force as an instrument of national policy, of computer network attack. Analysis centers on the United Nations Charter's prohibition of the use of force in Article 2(4), its Chapter VII security scheme, and the inherent right to self-defense codified in Article 51. Concluding that traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by CNA, the Article proposes an alternative normative framework based on scrutiny of the consequences caused by such operations.*

TABLE OF CONTENTS

	About the Author	2
	About the Institute for Information Technology Applications	2
	Abstract	3
	Introduction	4
I.	Understanding Computer Network Attack	6
II.	Computer Network Attack as a Use of Force	10
III.	Responding to Computer Network Attacks with Force	22
IV.	Concluding Thoughts on the Appropriate Normative Framework	27
	Endnotes	32

Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework

INTRODUCTION

As the next millennium approaches, the global community's dependence on computers and the networks that connect them, such as the Internet, is growing exponentially. This dependency amounts to a significant vulnerability, for computer networks underlie key societal functions as diverse as finance, military command and control, medical treatment, and transportation. Great attention is already being placed on the methods and means by which computer network attacks ("CNA") might be conducted, and significant resources are being devoted to developing offensive and defensive CNA capabilities.

This Article explores the acceptability under the jus ad bellum, that body of international law governing the resort to force as an instrument of national policy, of computer network attack. Analysis centers on the United Nations Charter's prohibition of the use of force in Article 2(4), its Chapter VII security scheme, and the inherent right to self-defense codified in Article 51. Concluding that traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by CNA, the Article proposes an alternative normative framework based on scrutiny of the consequences caused by such operations. By contrast, the Chapter VII security regime is assessed as sufficiently flexible to adapt to the new threats represented by CNA. Finally, the Article argues for a rather restricted understanding of the right to self-defense, suggesting that it be limited to operations which are de facto armed attacks, or imminently preparatory thereto. The net result is a limitation on both state resort to CNA techniques which might threaten global stability and on individual responses which might themselves prove destabilizing.

The global community is fast becoming "wired." By the beginning of the next millennium some 100 million individuals will enjoy access to the Internet.[1] Indeed, over the past decade the number of users has almost doubled annually.[2] Today, students attend virtual universities continents away from their computer terminals; shoppers buy on-line from their living room, and lawyers perform complex legal research without ever opening a law book. More significantly, the use of computers, and the networks that link them to one another, has become far more than a matter of mere convenience—in some cases survival may be at stake. International air traffic control relies on linked computer nets, as do such diverse, and critical, functions as telephone operations, emergency response, medical record management, oil distribution, municipal sewage treatment, electrical generation, and railway switching.

Military reliance on computers has grown in lock-step fashion with reliance on computers in the civilian sector. Today, the United States Department of Defense (DOD) employs well over two million computers and operates more than ten thousand local area networks. Moreover, some two hundred command centers are computer-dependent. These figures do not account for the two million plus computer users that regularly do business with the DOD.[3] While the armed forces of other nations are less dependent on computer resources and connectivity than those of the United States, the trend towards

military computerization, with varying degrees of fervor, approaches universality. After all, the 1990-1991 Gulf War aptly demonstrated the determinative effect of technology, particularly computer-enabled logistics, communications, intelligence, and force application, on the modern battlefield. It was a lesson lost on few military thinkers or operators.[4]

Paradoxically, most capabilities carry within them the seeds of vulnerability, a truism well-illustrated by the new cyber dependencies, both civilian and military. Whether quantitative or qualitative in nature, the extraordinary advances made possible by breakthroughs in computer technology represent dangerous vulnerabilities exploitable by opponents ranging from economic, political, and military competitors, to terrorists and criminals. These threat sources are familiar. However, the unique nature of the cyber threats they pose differs in four interrelated ways from those traditionally faced. First, computer networks comprise a new target category. It is no longer necessary, for example, to physically destroy electrical generation facilities to cut power to a foe's command and control system; instead, the computer network that drives the distribution system can be brought down to accomplish the same result. Second, whereas the means of "attack" in centuries past usually presupposed the use of kinetic force, in the twenty-first century an attack may be nothing more than the transfer of cyber commands from one computer to others. Third, while the result of a cyber attack may be physical destruction, such as the "meltdown" of a nuclear reactor following interference with its control systems, it need not be. The objective may simply be to shut off a particular service or function (e.g., disrupting telecommunications) or to alter or misdirect data (e.g., unauthorized electronic funds transfer or transmittal of false intelligence information). Finally, cyber attacks stretch traditional notions of territorial integrity. In most cases they will not involve the crossing of political borders by any tangible instrument of the attacker, such as military forces, equipment, or projectiles.[5]

This article explores the jus ad bellum implications of one such cyber threat—"computer network attack"—in a state-on-state context. Computer network attack consists of "[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[6] After briefly setting forth the technical and doctrinal framework for CNA, analysis will turn to the issue this new potential technique of international coercion poses: When does a computer network attack conducted by, or on behalf of, a state constitute a wrongful use of force under international law? Though it is not the focus of this essay, a brief discussion of the responses available to a state victimized by CNA will follow.

Such issues arise in two scenarios. In the first, State A conducts CNA operations against State B with no intention of ever escalating the conflict to the level of armed engagement. The advantages gained through the CNA are ends in themselves. In the second scenario, State A conducts CNA operations in order to prepare the battle space for a conventional attack. The goal is to disorient, disrupt, blind, or mislead State B so as to enhance the likelihood that conventional military operations will prove successful.

Although not limited to the security scheme set forth in the United Nations Charter, analytical emphasis will be placed on the prohibition on the use or threat of force in Article 2(4), Chapter VII's authorization of community responses in the face of aggression, and the right to self-defense codified in Article 51. The intent is to survey the existing normative architecture for prescriptive fault lines, those points where the jus ad bellum, as understood in prevailing cognitive paradigms, fails to adequately

safeguard and foster shared global values.[7] To the extent such fault lines are identified, suggestions as to how either causative normative lacunae might best be filled, or cognitive paradigms might profitably shift, will be offered for consideration. The Article will conclude with tentative thoughts on the policy implications of differing approaches to addressing the fault.

I. Understanding Computer Network Attack

Computer network attack is but one form of a relatively new category of warfare, information operations ("IO")[8]. Information operations comprise "[a]ctions taken to affect adversary information and information systems while defending one's own information and information systems."[9] The term must be understood very expansively. For instance, the United States military defines information as "facts, data, or instructions in any medium or form" and an information system as the "entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[10] Thus, information operations would encompass, among an array of other activities, virtually any nonconsensual actions intended to discover, alter, destroy, disrupt, or transfer data stored in a computer, manipulated by a computer, or transmitted through a computer network. To the extent these operations, whether occurring during times of peace or armed conflict, intend interference with a country's national defense by targeting defense premises or resources, including human and natural resources, they constitute "sabotage."[11] It should also be noted that the term "information warfare" ("IW") is often incorrectly used as a synonym for "information operations." In fact, IW accurately refers only to those information operations conducted during times of crisis or conflict intended to effect specific results against a particular opponent.[12] Thus, IW would not include information operations occurring during peacetime.

As suggested, IO is subdivided into defensive and offensive information operations.[13] CNA lies within the latter grouping, together with such varied activities as military deception,[14] psychological operations,[15] electronic warfare,[16] physical attack, and special information operations.[17] Its defining aspect is that it operates on data existing in computers or computer networks. That being so, computer network attack cuts across many categories of offensive IO—its intended result, for instance, might be deception or psychological effect. It is a technique, rather than a particular genre of objective. CNA operations can be used to facilitate strategic, operational, and tactical ends.[18] Further, because physical destruction seldom results from CNA, decision-makers find it a particularly attractive option in situations short of armed conflict.[19]

CNA techniques vary widely. Perhaps best known is the transmission of computer viruses into an adversary's computer network to destroy or alter data and programs. Logic bombs can also be introduced that sit idle in a system, awaiting activation at the occurrence of a particular event or set time. A logic bomb might be set to "explode" upon the call-up of reserve forces. Other techniques for disrupting information systems range from simply flooding it with false information to using "sniffer" programs to collect access codes that allow entry into a targeted system. In some cases, such attacks may occur without revealing the source, or even the fact, of the attack. In others, the identity of the attacker might be "spoofed" so as to convince the victim that the attack originated elsewhere.

Hypothetical examples of CNA, some realistic, others stretching credulity, abound in the literature. Consider just a few.

> (1) Trains are misrouted and crash after the computer systems controlling them are maliciously manipulated.[20]
> (2) An information blockade is mounted to limit the flow of electronic information into or out of a target state.[21]
> (3) Banking computer systems are broken into and their databases corrupted.[22]
> (4) An automated municipal traffic control system is compromised, thereby causing massive traffic jams and frustrating responses by emergency fire, medical, and law enforcement vehicles.[23]
> (5) Intrusion into the computer system controlling water distribution allows the intruder to rapidly open and close valves. This creates a hammer effect that eventually causes widespread pipe ruptures.[24]
> (6) A logic bomb set to activate upon initiation of mass casualty operations is imbedded in a municipal emergency response computer system.

Lest such scenarios seem implausible, computer networks have already proven remarkably vulnerable. For instance, the Defense Information Systems Agency (DISA) identified fifty-three attacks on military and DOD systems in 1992. By 1995 that number had grown to 559, and an astonishing fourteen thousand incidents are anticipated in 1999. In addition, DISA estimates that only one attack in 150 is detected.[25] In what is perhaps the best known incident, two hackers penetrated the Air Force's Rome Laboratory in 1994 by using software that allowed them to appear legitimate. The intruders entered the system over 150 times, established links with foreign Internet sites, copied sensitive data, and attacked other linked government facilities and defense contractor systems.[26]

Particularly problematic is the fact that the source of the vulnerability is the very interconnectedness that renders networks so powerful. Most significantly, interconnectivity exacerbates the consequences of CNA due to the likelihood of reverberating effects. An incident in 1996 illustrates how this phenomenon can occur. When a single power line in Oregon short-circuited, other power lines were forced to assume its load. Unable to cope with the increased demand, they too became overloaded and were shut down. The situation continued to snowball. By the time it was brought under control, a power blackout had spread to portions of fifteen states, as well as parts of Canada and Mexico.[27] Although not the product of a computer network attack, an identical result could easily have been caused by one.

The danger is that interrelationships cut across critical components of the national infrastructure. The Office of Science and Technology Policy, likening it to Mrs. O'Leary's cow and the Great Chicago Fire, highlighted this dilemma in an assessment of infrastructure vulnerability:

> The public telephone network, for example, relies on the power grid, the power grid on transportation, and all the sectors on telecommunications and the financial structure . . . . Most of today's cybernetic networks are actually combinations of networks, interconnected and interdependent. Interactions among these subsystems are critical to overall network performance, indeed they are the essence of network performance. Because the system also interacts with the real world environment, the

> interactions among subsystems are not necessarily predictable and sequential, like the steps of an assembly process, but can be essentially random, unsynchronized, and even unanticipated.[28]

Obviously, this complex national infrastructure web contains within it the likeliest CNA targets, both because of its national import, and because it offers an opponent countless avenues of attack. Our energy, communications, industrial, financial, transportation, human services, and defense systems are brimming with computer dependencies.[29] Predictive efforts centering on potential targets and the methods that might be used to attack them lie at the core of defensive planning (and offensive brainstorming). Although such labors at times approximate random speculation, consider a representative attempt in the form of a notional list of the "Top 10" Information Warfare targets:

> 1. Culpeper, Virginia electronic switch which handles all Federal funds and transactions;
> 2. Alaska pipeline which currently carries 10 percent of all U.S. domestic oil;
> 3. Electronic switching system which manages all telephones;
> 4. Internet;
> 5. Time distribution system;
> 6. Panama Canal;
> 7. Worldwide Military Command and Control System (WMCSS);
> 8. Air Force satellite control network;
> 9. Strait of Malacca, the major maritime link between Europe-Arabian Peninsula and the Western Pacific and East Asia;
> 10. National Photographic Interpretation Center (Washington).[30]

Of course, these are information warfare targets designed to enhance an attacker's relative military position in times of crisis or conflict. Target sets would certainly differ for CNA conducted as part of a peacetime operation not intended to prepare the battle space for future conflict. However, the list illustrates specific examples of targets that serious thinkers have contemplated. Actual targets would, of course, depend on the overall political-military objective sought by the attacking state.

The emerging information age generates new vulnerabilities that are likely to be exploited. Opponents of developed, first-world states cannot hope to prevail on the battlefield, or even in the boardroom. The technological and fiscal wherewithal of the developed states underlies an unprecedented level of military and economic supremacy. Moreover, as between these preeminent states (primarily the United States, its NATO allies, and Japan), the likelihood of armed conflict is *de minimus*. Thus, opponents of any particular state cannot hope to turn to a peer competitor of that state for support.

Facing these realities, a lesser-advantaged state hoping to seriously harm a dominant adversary must inevitably compete asymmetrically. It must seek to counter the strengths of the opponent not head-on, but rather, circuitously, employing unorthodox means to strike at centers of gravity. For instance, possession of weapons of mass destruction (WMD) can offset conventional military weakness. This is precisely why the United Nations Security Council takes the UNSCOM effort to deprive Iraq of WMD so seriously. Iraq cannot possibly hope to successfully confront the U.S. and its allies on the battlefield, but a credible threat to employ chemical or biological weapons in pursuit of national objectives would give it disproportionate (and malevolent) influence on the world scene. Similarly, asymmetry also under girds most state or state-sponsored

terrorism. It presents a relatively inexpensive means of striking a superior opponent in a very visible, yet relatively cost-free manner.[31]

CNA offers analogous asymmetrical benefits. In the first place, and as will be explored infra, in many cases a computer network attack will either not merit a response involving the use of force, or the legality of such a response will be debatable (even if the victim is able to accurately identify the fact, much less the source, of attack). Thus, because of the potentially grave impact of CNA on a state's infrastructure, it can prove a high gain, low risk option for a state outclassed militarily or economically. Moreover, to the extent that an opponent is militarily and economically advantaged, it is probably technologically-dependent, and, therefore, teeming with tempting CNA targets.

To further complicate matters, the knowledge and equipment necessary to mount a computer network attack are widely available; CNA is quite literally "war on the cheap." One expert has asserted that with one million dollars and twenty individuals, he can "bring the U.S. to its knees."[32] Another maintains that the defense information infrastructure (DII) can be disrupted for weeks by ten individuals with $10,000, while still others claim that for $30,000,000, one hundred individuals could so corrupt the country's entire information infrastructure that recovery would take years.[33] To place these figures into context, a single F-16 aircraft cost $26,000,000 in fiscal year 1997.[34] Unfortunately, the ability to conduct such operations is widespread. The President's Commission on Critical Infrastructure Protection has projected that by the year 2002, some nineteen million individuals will have the know-how to launch cyber attacks.[35] Today, over 120 countries are in the process of establishing information operations competence.[36] In particular, the Chinese have discovered information *warfare*, and organized research in the subject proceeds apace.[37] So too, not surprisingly, has the United States. Each of the armed services, as well as the Central Intelligence Agency, currently operates an information operations center.[38]

The centrality of information assets to national security, and therefore the need to safeguard them from CNA, cannot be overstated, a point well-recognized in official doctrine. The U.S. National Security Strategy for 1997, states that:

The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and technologies are being developed and employed to protect and defend against these vulnerabilities; we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well.[39]

Similarly, the most recently published National Military Strategy provides:

> Success in any operation depends on our ability to quickly and accurately integrate critical information and deny the same to an adversary. We must attain information superiority through the conduct of both offensive and defensive information operations. . . . Superiority in these areas will enable commanders to contend with information threats to their forces, including attacks which may originate from outside their area of operations. It also limits an adversary's freedom of action by disabling his critical information systems.[40]

In light of this centrality, jus ad bellum issues loom large. The information infrastructure and its multitudinous components comprise an attractive target set, and because of the ease with which CNA can be conducted, a critical, and difficult to defend, vulnerability. It is to the legal milieu in which such operations might occur that analysis shall now turn.

II. Computer Network Attack as a Use of Force

As noted, any number of purposes might motivate a state to conduct computer network attacks. Perhaps the CNA is designed to lay the groundwork for a subsequent conventional attack. Alternatively, it may be intended to stand alone, to cause damage and disruption without any desire to facilitate latter traditional military operations. Regardless of its aim, normative evaluation of the actions that occur will center on whether or not the actions constituted a wrongful use of force, or threat thereof, in violation of international law.

Article 2(4) of the UN Charter expresses the key prescription in international law regarding the use of force. By that provision, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[41] Purposes of the United Nations expressly cited in the Charter include the maintenance of international peace and security.[42] Therefore, uses (or threats) of force which endanger international stability fall within Article 2(4)'s prescriptive envelope. It is a prohibition reiterated in numerous international instruments, both binding and aspirational.[43] Lest the provision be misinterpreted, it is important to recall that Article 2(4) is prohibitive rather than remedial in nature. It does not, in and of itself, authorize any response to a use or threat of force. Rather, the Charter delineates the bases for response to the wrongful use of force, as will be discussed infra, in Chapters VI and VII. Article 2(4) merely serves to render particular uses of force wrongful in the Charter scheme.

Before turning to the specific query of when CNA might violate Article 2(4), it is first necessary to briefly consider the reach of Article 2(4).[44] The most significant issue surrounds the seemingly restrictive phrase "territorial integrity or political independence, or in any other manner inconsistent with the Purposes." Are there uses of force not otherwise authorized within the Charter that fall beyond Article 2(4)'s gamut because they do not threaten the territorial integrity or political independence of a target state or otherwise violate some specifically articulated prohibition found elsewhere in the Charter? Although the precise wording of the article generated much controversy as the Charter was being negotiated,[45] the mainstream view among international law experts is that the "other manner" language extends coverage to virtually any use of force not authorized within the Charter.[46] Thus, applying the prevailing positivist approach, analysis of use of force scenarios proceeds from the premise that an authorization for the use has to be found within the four corners of the Charter, not from the postulate that force is permissible unless a specific Charter prohibition thereon applies.[47] In the CNA context, this understanding would limit the scope of inquiry to whether the operation amounts to a use of force. Of course, the meaning of "force" may prove a matter of some dispute, as may the precise boundaries of the Charter's use of force sanctions, but if a CNA operation constitutes force, it will be deemed wrongful unless Charter-based. No further analysis is necessary.

Although textually sound, the positivist approach fails to reflect the realities underlying uses of force. It evidences misguided fidelity to the failed constitutive endeavor to establish a Charter security schema that would generally dispense with the need for unilateral uses of force, except in aberrant situations necessitating immediate self-defense. The envisioned normative architecture presupposed an effective enforcement mechanism—collective response under Security Council control—that has only slowly, and somewhat haphazardly, begun to be realized in the last decade. Absent an authoritative coercive enforcement mechanism, strict adherence to the plain text meaning of Article 2(4) can actually operate as a counterpoise to the Charter's world order aspirations. Specifically, adherence to a textual interpretation of the Charter security regime only allows either collective responses under Security Council mandate or defensive actions. During the Cold War, the Security Council was rendered impotent by bipolar competition. Despite the demise of bipolarity, the international community continues to struggle to forge consensus in the face of glaring acts of aggression, breaches of peace, or threats to peace. Inflexible understandings of Article 2(4)'s relationship to uses of force risk foreclosing unilateral or multilateral responses to deleterious situations that desperately demand community action, but upon which the Security Council has failed to act.

Fortunately, the international community has not allowed itself to be crippled by the relative desuetude of the Charter security system. On the contrary, in many cases states have responded to situations, either individually or in concert, in which community interests were served by taking coercive measures not specifically provided for in the Charter. Such incidents combine to map out a complex operational code as to those coercive acts the international community, or at least the politically relevant members thereof, accepts as lawful. Over a decade ago, Professor Michael Reisman identified nine basic categories of unilateral uses of force which enjoy some degree of community support:

> [S]elf-defense, which has been construed quite broadly; self-determination and decolonization; humanitarian intervention; intervention by the military instrument within spheres of influence and critical defense zones; treaty-sanctioned interventions within the territory of another State; use of the military instrument for the gathering of evidence in international proceedings; use of the military instrument to enforce international judgements; and counter measures, such as reprisals and retorsions.[48]

The majority of these actions would be difficult to justify under the Charter, absent a strained interpretive effort.

As Professor Reisman notes, the categories themselves are not determinative.[49] Instead, every threat or use of force is evaluated on its own merits based upon the context in which it occurs. Thus, for example, while the operational code acknowledges the lawfulness of humanitarian intervention in certain circumstances, in others it might be deemed unlawful—the operational code is contextual. Moreover, the categories in which uses of force are sometimes considered appropriate evolve. New categories, such as use of the military in cross border counter-terrorist operations, may emerge, while shifts in the nature and effectiveness of the Charter security scheme may diminish the acceptability of others, such as the unilateral use of the military instrument to gather evidence. Many criteria of lawfulness operate synergistically to contribute to the final assessment of legality, such as the imminence and severity of the situation being

addressed, less coercive or less violent alternatives and the viability of community responses. Ultimately, though, such extra-Charter uses of force will fall outside the operational code if they fail to advance shared world order values. The point here is not to index the operational code vis-à-vis uses of force, but rather to simply highlight the fact that a Charter analysis cannot be performed in isolation of the constantly developing and evolving operational code.[50]

Article 2(4) continues to enjoy predominant prescriptive valence, and it remains appropriate to view the provision as a general prohibition on non-Charter uses of force. That said, it must be recognized that certain forceful acts that lie outside the narrow options available in the Charter nevertheless comport with the operational code. A useful approach may well be to apply a rebuttable presumption to uses of force not specifically consistent with the Charter security system. A presumption of unlawfulness would attach to any such use. The burden would then shift to the actor to justify its actions within the relevant international community.

Given this analytical framework, the dispositive question is whether CNA constitutes use of force. Since the drafting of the UN Charter, the reach of the term "force" has proven contentious. The Vienna Convention on the Law of Treaties sets forth the core interpretive principle that international instruments are to be interpreted "in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and scope."[51] But what is the plain meaning of the term "force"? Does it only extend to "armed" force, i.e. force applied by military units, or does it encompass other forms of coercion? In addressing this issue, some commentators point to the Charter itself,[52] an approach consistent with the Vienna Convention's inclusion of a treaty's preamble, text, and annexes in its "context."[53] For instance, the Preamble includes among Charter purposes the goal that "armed force . . . not be used save in the common interest . . . " If the Article 2(4) prohibition were intended to extend beyond armed force, then presumably the preamble, for reasons of internal consistency, would not have included the term "armed." After all, the Charter's articles are designed to effectuate its preambular aspirations. Thus, preambular terminology is logically interpreted more broadly than that contained in the articles. The wording of Article 44 further supports a restrictive interpretation. It states, "When the Security Council has decided to use force it shall, before calling upon a Member not represented to provide armed forces . . . " "Force" appears, as in Article 2(4), without the qualifier "armed," but, as demonstrated by the reference to "armed forces," clearly contemplates that the force used be armed.

The Charter uses the term "armed force" twice,[54] a fact which might seem to suggest the drafters intended to distinguish it from unqualified force after all. However, both cases involve Chapter VII enforcement, in which armed force is but one of multiple options available to the Security Council in responding to threats to the peace, breach of the peace, or acts of aggression. Read in context, they clearly refer to a particular point along the continuum of coercion. By contrast, because Article 2(4) precludes nothing but "force," there was no need to distinguish it through qualification.

While textual analysis is often telling, it is based on the somewhat suspect premise that a diverse group of diplomatic teams was thoroughly aware of the subtle nuances of language. This is so despite the fact that many members of the teams do not share English (or for that matter any language of the other authoritative texts—Chinese, French, Russian, and Spanish) as their first language.[55] Of course, negotiating teams

do obsess over terminological precision in order to avoid committing their state to unintended and undesired obligations. However, should ambiguity or obscurity remain, interpretive recourse may be made to "the preparatory work of the treaty and circumstances of its conclusion."[56]

In the case of Article 2(4), the *travaux préparatoires*[57] do shed considerable light on the subject. At the San Francisco Conference, the Brazilian delegation submitted amendments to the Dumbarton Oaks proposals that would have extended Article 2(4)'s range to economic coercion.[58] Though the proposition received a majority vote in committee, the Conference declined adopting it by a vote of 26-2.[59] Thus, analysis based on both UN Charter travaux and text leads to an interpretation excluding economic, and for that matter political, coercion from Article 2(4)'s prescriptive sphere.

Other international instruments of the time also used the term "force" without qualification.[60] In none of them does any support for inclusion of economic or political pressure appear. In fact, the terminological approach in one of the key constitutive documents of the time implies just the opposite. The Charter of the Organization of American States (as subsequently amended) avoids use of the naked term "force" altogether, instead separately referring to "armed force" and "coercive measures of an economic or political character."[61] Its drafters appear to have been sensitive to the normative import of the distinction, an unsurprising fact in light of Brazil's membership in the organization.[62]

In fairness, the restrictive interpretation has not enjoyed universal acceptance. The desire for a broader definition resurfaced twenty-five years after the San Francisco Conference during the drafting of the General Assembly's Declaration on Friendly Relations. The Declaration expresses the use of force prohibition in terms identical to Article 2(4).[63] During committee handling of the draft, differences of opinion again arose over whether the term "force" should extend to "all forms of pressure, including those of a political or economic character, which have the effect of threatening the territorial integrity or political independence of any State."[64] Most Western States sought to limit the expression to armed force, in some cases linking the prohibition to the right to respond in self-defense pursuant to Article 51 of the Charter to an armed attack. In contrast, the bulk of African and Asian nations advocated a purpose-based interpretive analysis. By their reasoning, a desire to assure the political independence of States through protection of sovereign prerogative and territorial inviolability permeated Article 2(4). To the extent that economic and political coercion constituted a threat to those principles, the article, as well as the Declaration, should be interpreted to preclude such misdeeds. For proponents, interpretative endeavors, particularly when text is ambiguous, should not be foreclosed by travaux, but rather should reflect the underlying purposes of the article in the current international context. Latin American countries split on the issue.

Ultimately, the debate proved impossible to resolve—the Declaration's Principles, and the textual explication thereto, do not directly address the differences. However, much of the explanation of the Principle prohibiting resort to force is cast in terms relevant only to armed force.[65] That the Declaration fails to cite economic or political measures in the Principle on the use of force, but does so with regard to the Principle imposing a duty not to "intervene in matters within the domestic jurisdiction of any State,"[66] strengthens the restrictive argument. Tellingly, a second General Assembly Resolution on the subject, this one issued in 1987, takes an analogous approach. In the Declaration on the

Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, "armed intervention" is tied to "interference or attempted threats against the personality of the State or against its political, economic and cultural elements," whereas economic and political coercion are cited in the context of "the subordination of the exercise of . . . sovereign rights" and securing "advantages of any kind" from the target state.[67] Again, while the Declaration does not definitively resolve the reach of the term "force," its general tenor, and the varying contexts in which armed, economic, and political coercion arise, suggest that although economic and political coercion may constitute threats to international stability and therefore are precluded by the principle of non-intervention (discussed infra), the concept of the use of force is generally understood to mean armed force.[68]

The foregoing analysis shows that the prohibition of the threat or use of force includes armed, but not economic or political coercion.[69] However, it does not demonstrate that the borders of "force" precisely coincide with armed force, i.e., physical or kinetic force applied by conventional weaponry. This reality has only recently proven of applicative import. Until the advent of information operations, most coercion could be handily categorized into one of several boxes, for few coercive options existed that could not be typed as political, economic, or armed in nature. Because there was little need to look beyond these genera, discourse about the lawfulness of State coercion, as illustrated supra, tended to revolve around them. If the act in question fell within the armed force box, it violated the prescription banning the use of force; if not, questions of legality had to be resolved by looking elsewhere.[70]

On rare occasions, the relatively bright line test for wrongful use of force proved inutile. For instance, in the Nicaragua Case the International Court of Justice (ICJ), held that:

> [W]hile arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua . . . does not itself amount to a use of force.[71]

Assuming the Court accurately characterized the state of the law, the dimensions of the armed force box grew slightly. In what was tantamount to an application of agency theory, the Court determined that force apparently includes actively and directly preparing another to apply armed force, but not merely funding the effort. Nevertheless, despite the subtle shift in the understanding of force, prescriptive ratiocination continues to transpire within a familiar paradigm, that of distinguishing armed force from other tools of coercion.

At least since promulgation of the Charter, this use of force paradigm has been instrument-based; determination of whether or not the standard has been breached depends on the type of the coercive instrument—diplomatic, economic, or military—selected to attain the national objectives in question. The first two types of instruments might rise to the level of intervention, but they do not engage the normatively more flagrant act of using force. However, despite instrument classing, in actual practice it does not follow that coercive acts involving armed force necessarily operate at counter-purposes with community values (they are condoned when consistent with the operational code). Even when they do, it is not always the case that they do greater

violence thereto. For instance, a temporally and spatially limited border incursion is probably a lesser threat to either international peace and security or the right of states to conduct their affairs free from outside interference than was the 1973-1974 Arab oil embargo.[72] Yet, the prescriptive framework would proscribe the former, but not the latter.[73]

In order to understand the distinction, one must first inquire into why the limitation exists at all. International law regarding coercion seeks to foster or frustrate consequences. Although, as noted in the discussion of operational codes, normative architectures evolve over time as community aspirations shift in one direction or another, certain shared community values, albeit often aspirational, permeate world order prescription. They include, *inter alia*, physical survival and security for both individuals and the tangible objects on which they rely, human dignity (particularly that expressed in human rights norms), social progress and quality of life, and "the right of peoples to shape their own political community."[74] In a sense, these aspirations echo a human hierarchy of need. International law seeks to advance them to a degree largely determined by both their position in the hierarchy of need and the nature of the systemic constraints that the international system imposes on their pursuit.

The primary constraint, the determinative reality, is that these aspirations must be pursued within a state-based international structure. This structure contains many obstacles, not the least of which is interstate rivalry rift with zero-sum thinking.[75] The UN Charter reflects this understanding by including in its purposes the maintenance of international peace and security, development of friendly relations among nations, achievement of international cooperation in solving international problems, and harmonization of the actions of nations.[76] While these appear to be goals in and of themselves, they are actually intermediate goals in the attainment of the ultimate ends just articulated. They are community value enablers.

The prohibition on the use of force is designed to advance these intermediate objectives (and occasionally the ultimate aims) by restricting those acts most likely to endanger them—uses of force. In fact, the international community is not directly concerned with the particular coercive instrumentality used (force in this case), but rather the consequences of its use. However, it would prove extraordinarily difficult to quantify or qualify consequences in a normatively practical manner. Undesirable consequences fall along a continuum, but how could the criteria for placement along it be clearly expressed? In terms of severity? Severity measured by what standard of calculation? Harm to whom or what?[77]

The difficulty in looking to consequences themselves as criteria for calculating lawfulness led the Charter drafters to use prescriptive short-hand to achieve their goals. Because force represents a consistently serious menace to intermediate and ultimate objectives, the prohibition of resort to it is a relatively reliable instrument-based surrogate for a ban on deleterious consequences. It eases the evaluative process by simply asking whether force has been used, rather than requiring a far more difficult assessment of the consequences that have resulted.

Of course, the use of force can cause widely divergent results depending on the weapon used, scale of attack, and nature of the target, as can economic coercion, which may result in everything from financial uneasiness to the collapse of an economy. Nevertheless, instrument-based evaluation is merited in the case of the former, but not

the latter, by virtue of its far greater consequence-instrument congruence. Armed coercion usually results in some form of physical destruction or injury, whereas economic (or political) coercion seldom does. Additionally, the risk of an escalating conflict from a use of force ordinarily exceeds the risk from economic or political coercion because force strikes more directly at those community values at the top of the human hierarchy of need, in particular survival. The fact that the consequences of the use of force are almost immediately apparent, whereas economic or political consequences, although severe, emerge much more slowly, and thereby allow opportunity for reflection and resolution, compounds the danger of escalation. An even more basic problem is pinning down the cause and effect relationship when applying economic and political coercion. During the time lag between the initiation of the coercion and the emergence of consequences, intervening factors may enter the picture without which the consequences would not have occurred.

Because the results of applying economic and political instruments generally constitute lesser threats to shared community values, the use of force standard serves as a logical break point in categorizing the asperity of particular coercive acts. Any imprecision in this prescriptive short-hand is more than outweighed by its clarity and ease of application.

What matters, then, are consequences, but for a variety of reasons prescriptive shorthand based upon the instrument involved classifies coercive acts into two categories—those the community most abhors (force), and all others (which may in themselves violate less portentous community prescriptions). Computer network attack challenges the prevailing paradigm, for its consequences cannot easily be placed in a particular area along the community values threat continuum. The dilemma lies in the fact that CNA spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g., shutting down an academic network temporarily) to physical destruction (e.g., as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g., shutting down power to a hospital with no back-up generators). It can affect economic, social, mental, and physical well-being, either directly or indirectly, and its potential scope grows almost daily, being capable of targeting everything from individual persons or objects to entire societies.

Note that Article 41 of the Charter cites “interruption of . . . communication” as a “measure not involving armed force.”[78] Certainly, some forms of computer network attack would fall in the ambit of this characterization. However, many forms would not. More to the point, the Charter drafters did not contemplate CNA. Therefore, to reason that CNA is a “measure not involving armed force” by virtue of Article 41 is over-reaching. So how should computer network attack best be characterized? As a use of armed force? As force? As some nascent modality of inter-State coercion which exists in a normative void?

One narrow category of computer network attack is easily dealt with. CNA specifically intended to directly cause physical damage to tangible property or injury or death to human beings is reasonably characterized as a use of armed force and, therefore, encompassed in the prohibition. Thus, in the examples above, the pipeline destruction and the shutting of power to the hospital are examples of CNA which the actor knows can, and intends to, directly cause destruction and serious injury. Armed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused, specifically physical damage and human injury.

Instrumentalities that produce them are weapons. There is little debate about whether the use of chemicals or biologicals falls within the meaning of armed force, even though the means that cause the injury or death differ greatly from those produced by kinetic force.[79] Similarly, there was little doubt that neutron bombs constitute weapons, nor has controversy over the classification as weapons of the new varieties of non-lethals (many of which do not release kinetic energy as a mode of effect) surfaced.[80] That computer network attack employs electrons to cause a result from which destruction or injury directly ensues is simply not relevant to characterization as armed force. The dilemma lies beyond this limited category of computer network attacks. How should computer network attacks which do not cause physical damage or injury, or do so indirectly, be classed vis-à-vis the prohibition on the use of force?

Unless the international community is willing to adopt a de novo scheme for assessing the use of inter-state coercion, any justification or condemnation of CNA must be cast in terms of the use of force paradigm. In that computer network attack cuts across the instrument-based distinction employed as prescriptive short-hand, it becomes necessary to shift cognitive approach if one wishes to continue to operate within the existing framework. The key to doing so lies in revisiting the "force" box. As the discussion has illustrated, the controversy surrounding the meaning of the term was not so much whether the concept was limited to armed force, but rather whether it included economic coercion. To the extent that the qualifier "armed" was cited, it was done in order to counter the argument for extension. There was no need to look beyond armed force because intermediate forms of coercion such as CNA were not generally contemplated. Yet, the holding of the ICJ in the Nicaragua Case with regard to arming and training the contras suggested that other forms of "force" were not necessarily excluded. Therefore, the use of force line must lie somewhere between economic coercion and the use of armed force. The question becomes how to locate the point of demarcation, at least with regard to this new genre of coercion.

Perhaps the best approach is to start by reflecting upon the underlying motivation for the instrument-based distinctions: consequences. This is an imprecise endeavor, for, as discussed, the instruments do not precisely track the threats to shared values which, ideally, the international community would seek to deter. Nevertheless, if commonalities between typical consequences for each category can be articulated, perhaps CNA can be classed according to consequence affinity with the current prescriptive distinguishers.

Economic and political coercion can be delimited from the use of armed force by reference to various criteria. The following number among the most determinative:

1) Severity: Armed attacks threaten physical injury or destruction of property to a much greater degree than other forms of coercion. Physical well-being usually occupies the apex of the human hierarchy of need.
2) Immediacy: The negative consequences of armed coercion, or threat thereof, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodation is hampered in the former case.
3) Directness: The consequences of armed coercion are more directly tied to the *actus reus* than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty.

4) Invasiveness: In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability.
5) Measurability: While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force.
6) Presumptive Legitimacy: In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self-defense. The cognitive approach is prohibitory. By contrast, most other forms of coercion—again in the domestic and international sphere--are presumptively lawful, absent a prohibition to the contrary. The cognitive approach is permissive. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a very generalized rule).

These consequence commonalities can serve as the ties between CNA and the prevailing instrument-based prescriptive shorthand.[81] By this scheme, one measures the consequences of a computer network attack against the commonalities to ascertain whether they more closely approximate consequences of the sort characterizing armed force or whether they are better placed outside the use of force boundary. This technique allows the force box to expand to fill lacunae (that became apparent upon the emergence of coercive possibilities enabled by technological advances) without altering the balance of the current framework—the growth is cast in terms of the underlying factors driving the existing classifications.

How might this technique operate? In determining whether an opponent's computer network attack (or threat thereof) fell within the more flexible consequence–based understanding of force (or whether an action being considered by one's own information warriors does), the nature of the act's reasonably foreseeable consequences would be assessed to determine whether they resemble those of armed coercion. If so, extension of the use of force prohibition to the act would be justified. If not, wrongfulness under international law would have to be determined by resort to prescriptive norms other than that prohibiting force.

Consider two apposite examples. In the first case, computer network attacks disable a busy air traffic control (ATC) system during horrendous weather. An airliner crashes and deaths result. No kinetic force has been used to destroy the airliner, but CNA was plainly the proximate cause of the tragedy. This action would be considered a use of force. The severity of the consequences, multiple deaths and physical destruction, rises to a level equal to that of armed coercion. The technique did not permit sufficient opportunity to defuse the crisis before the consequences occurred, and, although CNA did not directly target the aircraft's on-board systems, the crash would not have occurred but for the attack on the ATC assets. Furthermore, in order to cause the damage, signals had to be transmitted across political borders. The consequences of the attack are easily measurable (in terms of human and property loss), and, although attempts to harm others through their computers and computer networks is a relatively new

technique, there is a growing body of law in many countries criminalizing such activities.[82]

Contrast this analysis with that addressing an attack on a university computer network designed to disrupt military related research occurring in campus laboratories. Severity, considered in the context of shared values, falls significantly below that of armed coercion. No physical damage or measurable suffering occurs, at least in the short term. The desired outcome, diminished capability on the battlefield, is remote from the act, and it is indirect in that it will depend on a number of indeterminacies—the ability to regenerate data, the possible existence of other research efforts moving towards the same conclusions, the likelihood the project would have been funded through entry into the inventory, etc. Although the transmission of the signal is intrusive and presumptively illegitimate, metering the consequences will prove difficult. In sum, the underlying nature of the consequences resulting from this particular information operation fails to sufficiently resemble that characteristic of uses of armed force. Extension of the instrument-based use of force distinguisher would be inappropriate.

It may appear torturous to use the prescriptive shorthand (instrument-based classification) as a point of departure, rather than simply ask to what degree the consequences of computer network attack threaten shared community values. One might simply look no further than the severity of consequences.[83] Indeed, at conferences and among those who have considered the subject in any depth, there is a tendency to take this stance when struggling with the dilemma of how to account for non-kinetically based harm with a system designed to regulate kinetic activities. The flaw in doing so lies in the fact that it calls for a new normative architecture altogether to handle such actions, an architecture that amounts to more than an interpretive dilation of the use of force standard. It would constitute a new standard.

By contrast, reference to the instrument-based shorthand facilitates greater internal consistency and predictability within the preexisting framework for inter-state coercion. It allows determinations on the inclusivity of the use of force to more closely approximate the current system than analysis based solely on consequentiality would allow. As a result, subscription by the international community is more likely, and application should prove less disruptive and controversial. This is not to say that greater focus on core objectives, on consequentiality in its pure form, is not to be sought. It is only a recognition that until the international community casts off its current cognitive approach, community values are, for practical reasons, best advanced in terms of that which is familiar and widely accepted.

It should be noted that schema-imbuing consequences, rather than acts, with normative valence are nothing new. In the *jus in bello*, consequence-based analysis predominates. The principle of proportionality, for instance, balances positive consequences (military advantage) against harmful ones (collateral damage and incidental injury).[84] Additionally, Protocol I to the Geneva Conventions prohibits starvation of civilians, causation of "widespread, long-term and severe damage" to the environment, and attacks on works and installations containing dangerous forces which "may cause the release of dangerous forces and consequent severe losses among the civilian population."[85] Similarly, the Environmental Modification Convention forbids the use of any hostile environmental modification technique that has "widespread, long-lasting or severe effects."[86]

More to the point, consequentiality arguably dominates analysis of inter-state coercion short of the use of force, for once an act slips out of the force box into a category containing other coercive methods, the issue of the instrument fades in favor of consequences, specifically the consequence of intervention in the affairs of other states. Of course, armed coercion can constitute intervention, but the modality of coercion rather than the fact of intervention is determinative. By contrast, in considering non-forceful coercion, the start point is whether it amounts to prohibited intervention. For instance, the Declaration on the Inadmissibility of Intervention provides that "[n]o State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind . . . ."[87] It is not the fact of economic coercion, but rather its consequence that matters. Thus, while certain techniques may be prohibited by a particular international agreement,[88] the encompassing norm is consequence-based.

Arguably the approach to CNA and the use of force suggested in this essay falls within the camp of "radical teleological interpretation," for ultimate purposes are being identified in order to lend prescriptive substance to a treaty provision.[89] Yet, this is not a case of crafting new prescriptions, but rather one of simply determining how to address activities not contemplated at the time the Charter was promulgated by resort to Charter norms. Clearly, had CNA posed a significant threat in 1945, the drafters would have crafted a standard against which it could be prescriptively measured. Moreover, because the Charter is the constitutive instrument of an international organization, flexibility in interpretive spirit is apropos. Such documents must remain malleable if the organization in question is to remain relevant to changing international circumstances. As one distinguished commentator has noted, "[T]his [flexible] approach has been used as a way of inferring powers, not expressly provided for in the relevant instruments, which are deemed necessary in the context of the purpose of the organization."[90]

Finally, since the approach is consequence, vice instrument, based, it will forfeit much of the clarity that the latter mode of analysis offered; more gray area cases will occur. This is particularly true in the absence of state practice, and the responses thereto necessary to permit an operational code to emerge from the fog of inter-State relations. In assessing individual instances of CNA, then, the question is how to resolve the unclear cases. Should a presumption operate in favor of inclusion or exclusion of CNA in the use of force box?

While policy concerns may impel a particular state towards one position or the other, the security framework of the Charter would be best effected by application of an inclusivity presumption. If the debate is about whether a particular information operation is or is not a use of force, then the consequences of that operation are likely such that they would be violative of the prohibition on intervention at any rate. The issue is probably not legality, but rather illegality by what standard. Therefore, to the extent that treaty prohibitions have any deterrent effect, inclusivity would foster shared community values. The contrary position would assert that labeling uncertain cases as a use of force would be destabilizing, for the victim would be more likely to respond forcefully. However, as to be discussed, it is not the use of force, but rather "armed attack" which gives a state the right to respond in self-defense. An operation that generates doubt as to its status under use of force typology would surely not rise to the level of an armed attack. Moreover, this position does not leave the international community remedy-less. Under Article 39,

the Security Council may mount forceful responses even to events that threaten the peace. Most gray area cases would at least rise to this level.[91]

The prohibition on the use of force enjoys normative valence beyond its Charter context. It also constitutes customary international law.[92] Customary law has both objective and subjective components: it must evidence consistent state practice over time by a meaningful group of states and *opinio juris sive necessitatis*[93] must exist.[94] In evaluating the actions of the United States in the Nicaragua case, the International Court of Justice held that a prohibition on the use of force did exist in customary law (and that the U.S. had violated it).[95] In light of both the Court's conclusory finding regarding state practice[96] and its heavy reliance on non-binding General Assembly Resolutions to establish the requisite opinio juris,[97] the legal reasoning underlying the judgment is suspect. Nevertheless, a majority of commentators concur in the ultimate finding that the prescription enjoys customary status.[98]

The problem in application of the customary standard to CNA is that the customary and Charter prescriptions, while similar, do not coincide. The ICJ itself acknowledged this point in the Nicaragua case when it opined:

> [O]n the question of the use of force, the United States itself argues for a complete identity of the relevant rules of customary international law with the provisions of the Charter. The Court has not accepted this extreme contention . . . . However, . . . the Charter gave expression in this field to principles already present in customary international law, and that law has in the subsequent four decades developed under the Charter to such an extent that a number of the rules contained in the Charter have acquired a status independent of it.[99]

While state consent to be bound by a treaty can be interpreted as consent to reasonable application of accepted rules of interpretation, the state practice and opinio juris requirements of customary international law may lead over time to divergence among formerly coincident norms. Treaty law is both more and less flexible than its customary law counterpart. On the one hand, it is flexible in its susceptibility to interpretation in accordance with evolving context; such context is consequential even in the absence of any shift in state practice (perhaps the opportunity for state practice has not presented itself). On the other hand, it is inflexible in the sense that the prescription itself is frozen beyond interpretation thereof; new norms require new consent. Customary law, by contrast, is unlimited in scope, but limited by the fact that it cannot react to evolving context absent practice and opinio juris.

Of course, customary law responds to change in some degree. For instance, the prohibition of the use of force would extend to employment of any new weaponry that fell within the general ambit of armed force, for in the same way that Article 2(4) always contemplated armed coercion, so too has the customary standard. Indeed, because the Nicaragua decision was based on customary international law, it is reasonable to extend the concept of force to the direct support (arming/training) of those who employ it. Nevertheless, there is no basis in state practice for extension beyond the immediate periphery of armed force. In particular, the absence of any significant CNA practice renders it inappropriate to do so. A customary norm may develop over time, but it does not exist at present. Neither practice, nor opinio juris, is in evidence.

This is not to say that CNA exists wholly beyond the customary international law governing the use of force. However, whereas the approach proposed in this essay would extend the treaty application to computer network attacks causing consequences which approximated the nature of those involving armed force, application of the customary norm to CNA would require it to be characterized as a new technique of armed force. In order to rise to this level, it must cause not analogous consequences, but identical results, specifically direct human injury or physical damage to tangible property. Thus, it must fall within the narrow category of computer network attacks that are appropriately characterized as an application of armed force.[100]

A final prospective point regarding customary international law lies in its greater potential scope. In responding to incidents of computer network attack, the effect of Article 2(4) can never advance beyond the interpretive boundaries of the existing use of force cognitive paradigm. However, over time a new customary norm may emerge that addresses CNA in and of itself, quite aside from its use of force implications. Such a norm may very well prove more restrictive than current prescriptions. At the present, the possibility is purely speculative.

Note that the prohibition on resort to force enjoys more than customary standing. It has been identified by both the International Law Commission[101] and the International Court of Justice[102] *as jus cogens*—"a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the character."[103] In essence, jus cogens norms are customary norms writ large, for they are not susceptible to avoidance through party consent (e.g., in the form of a later treaty). Given their customary character, the treatment of computer network attack in the jus cogens context mirrors that with regard to customary international law. Therefore, this specific peremptory norm extends to CNA rising to the level of a de facto use of armed force, but not to other forms of computer network attack.

Finally, although this essay centers on the use of force, it must be understood that the fact that a computer network attack does not violate peremptory, customary, or conventional use of force norms does not necessarily render CNA consistent with international law. In particular, an attack may amount to prohibited intervention in the affairs of other states. As noted by the ICJ in the Nicaragua case, "[t]he principle of non-intervention right of every sovereign State to conduct its affairs without outside interference . . . it is part and parcel of customary international law."[104] The obligation to refrain from intervention finds further expression in various General Assembly Resolutions, most notably the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty[105] and the Declaration on Friendly Relations.[106] CNA may be particularly appropriate for consideration in the context of intervention, due to its reliance on technology. Although the technology necessary to commit computer network attack is increasingly widespread, technologically advanced states still maintain an edge in their ability to use it. This disparity in access to the technique heightens its inadmissibility as a form of coercion.[107]

III. Responding to Computer Network Attacks with Force

While an in-depth analysis of the appropriateness of responding to computer network attack with force is beyond the purview of this essay, a brief outline of the subject is

useful to help place the use of force prohibition in context. With the exception of the operational code discussed supra, the framework for appropriate uses of force generally resides within the UN Charter. The Charter admits of only two situations allowing the use of force—Security Council authorized operations pursuant to Chapter VII and self-defense in accordance with Article 51.

Under Chapter VII, the Security Council has the authority to "determine the existence of any threat to peace, breach of peace, or act of aggression."[108] When the Council does so, it may call upon member states of the United Nations to apply "measures not involving the use of armed forces" to resolve the situation.[109] Note that the measures contemplated include "complete or partial interruption of . . . telegraphic, radio, or other means of communication," techniques likely to involve CNA. If non-forceful measures have proved inadequate, or if the Council believes that they would be futile, it may "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[110] Responses may include information operations falling into either the "not involving armed force" or "armed force" category, as long as they are conducted in accordance with methods and means limitations.[111] To the extent that the type of operation falls squarely within the mandate of the Security Council Resolution authorizing the action, the distinction between the two categories is not particularly relevant.

However, when does a computer network attack amount to a threat to peace, breach of peace, or act of aggression such that the Council may authorize a response by armed force? The answer can only be provided by the Security Council, for despite attempts by some states to imbue the provision with greater clarity during drafting of the Charter, the member states decided to allow the Council wide discretion by leaving the terms relatively undefined.[112]

In 1974, the General Assembly defined the term aggression as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any manner inconsistent with the Charter of the United Nations . . ".[113] Cast in terms of "armed" force, acts of aggression would only include those forms of CNA that rise to the level of armed force by virtue of their intent to cause direct damage or injury.[114] However, while all acts of aggression constitute breaches of the peace, or threats thereto, the obverse is not true; threats to the peace do not necessarily amount to aggression. Aggression is a pejorative term that implies fault; it imposes responsibility. A threat or breach of the peace, by contrast, may or may not be susceptible to the determination of blame, but nevertheless may merit a forceful community response. Moreover, while attaching responsibility by labeling an act aggressive requires that armed force have occurred, threatening or breaching of the peace need not. The mere fact that the peace is threatened is enough for the Security Council to engage the matter.

But what is meant by "peace"? Is it the absence of inter-state violence or does it envision something broader, such as human well-being or community cooperation? Article 1(2), for instance, speaks of "develop[ing] friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples . . . " in order to "strengthen universal peace."[115] Nevertheless, an overly expansive understanding of the concept would fly in the face of the sovereignty notions that pervade international law. That being so, the better interpretation seeks consistency with the Charter provision in which sovereignty concerns have already been balanced

against shared community values, Article 2(4)'s prohibition on the use of force. In the Charter context, then, peace may best be defined as the absence of the use of force, whether the use of that force is legitimate or not. Article 39 represents a value choice in favor of community, vice unilateral, replies to uses of force.

By the breach of peace standard, the Security Council could react forcefully pursuant to Article 42 to a computer network attack that amounted to a use of force as described above in the Article 2(4) context. Of much greater significance to information operations is the threat to the peace standard. It allows the Security Council to authorize a response by force to any situation that might provoke a breach of the peace (use of force). Legality, or lack thereof, of the prospective forceful response (the breach of the peace) to the provocation is not determinative as to whether a threat to the peace exists.[116] The question of threat is factual, not juridical. To complicate matters, the Security Council finds such threats with a fair degree of ease. For example, in 1991, the Council characterized fighting between the Yugoslavian government and the break-away states of Croatia and Slovenia as a threat to peace, most likely due to fear that this internal armed conflict might eventually risk involvement from outside the country.[117] Other examples of the Security Council finding threats to the peace in the last decade include, inter alia, the anarchy in Somalia,[118] civil war in Liberia,[119] and even the refusal of the Libyan government to turn over suspects in the Pan Am Flight 103 bombing.[120]

Given this liberality, many forms of computer network attack, whether a use of force or not, could comprise a threat to the peace. Each would have to be evaluated in context, the permutations of which are infinite—time, place, target, actor, consequence, etc. What might cause one target state to react forcefully at a certain time or in particular circumstances might be perceived as relatively unimportant by another. Certainly, any serious CNA conducted by contenders in long-standing global flash-points (e.g., India-Pakistan, Turkey-Greece) risks ignition. On the other hand, it is possible to envision computer attacks among major Western economic powers (perhaps in the form of economic espionage) that would clearly not threaten the peace if discovered. Reduced to basics, though, Security Council discretion in Chapter VII matters would be at its apex when determining whether a particular computer network attack amounts to a threat to the peace sufficient to justify a forceful community (or community-authorized) response.

Article 51 expresses the second UN Charter authorization of the use of force:

> Nothing in the present Charter shall impair the inherent right of individual and collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[121]

The sole authorization of unilateral use of force outside the Charter security system, this provision responds to the reality that the international community may not be able to react quickly enough to armed aggression[122] to forestall attack on a victim state. It therefore permits states and their allies to defend themselves until the international "posse" arrives pursuant to Chapter VII.

Note that Article 51 restricts a state's right of self-defense to situations involving armed attack, a narrower category of act than Article 2(4)'s use of force.[123] Although coercion not involving armed force may violate Article 2(4) and result in action under Article 39, it does not follow that states may also react unilaterally pursuant to Article 51. This narrowing plainly reflects the Charter's preference for community responses (e.g., even to threats to peace) over individual ones. In the case of a computer network attack, it is also a prudent approach due to the difficulty states may have in identifying the correct source of an attack.

Thus, faced with CNA that does not occur in conjunction with, or as a prelude to, conventional military force, a state may only respond with force in self-defense if the CNA constituted armed force by the standard enunciated supra for armed force, i.e., that it is intended to directly cause physical destruction or injury. The victim state could repair to the Security Council and allege that other acts of CNA threaten the peace and merit a Chapter VII response, but it could not respond forcefully thereto on its own accord. Additionally, computer network attacks falling short of armed attack might nevertheless violate Article 2(4)'s prohibition on the use of force, thereby subjecting the actor to international opprobrium, but not to a response in self-defense.

The foregoing analysis applies only to situations in which the computer network attack occurs in total isolation. What of computer network attacks launched to prepare the battle space? The possibilities abound. CNA disables intelligence gathering assets such as satellites. An opponent "attacks" the Global Positioning Satellite System (GPS) to confound targeting and maneuver. Computerized military medical records are corrupted to complicate provision of medical treatment upon the outbreak of hostilities. A logic bomb is implanted in the reserve activation system, programmed to operate upon call-up. Concerted CNA brings down large sections of the military communications network.

In none of these situations does the attack, in and of itself, constitute an armed attack. However, each may very well be an essential step in just such an attack. In certain circumstances, they would merit a forceful response. The prevailing standard maintains that an attack must be "imminent" before the right to self-defense matures. In the nineteenth century, Secretary of State Daniel Webster crafted the classic articulation of this "anticipatory" right with regard to the now famous Caroline incident. He opined that self-defense should "be confined to cases in which the necessity of that self-defense is instant, overwhelming, and leaving no moment for deliberation."[124] Mere preparation failed the test. Following World War II, the Nuremberg Tribunal spoke approvingly of the Caroline standard.[125]

Unfortunately, a conundrum surfaces in the application of the imminence criterion. Some commentators assert a high standard for imminence, reading the Caroline principle narrowly.[126] Indeed, on its face, it appears to impose a fairly restrictive temporal test. The force used in self-defense must occur just as the attack is about to be launched.

A better approach asks what the principle seeks to achieve. Obviously, it hopes to stave off violence so as to allow maximum opportunity for peaceful alternatives to work. However, at the same time, it recognizes that states need not risk destruction through inaction. The principle balances the desire to avoid inter-state violence against the right

of a state to exist unharmed. This being so, imminence is best understood as relative. For instance, as defensive options become more limited or less likely to succeed, the acceptability of preemptive action grows. A weak state may be justified in acting sooner than a stronger one, when facing an identical threat, simply because it is at greater risk in having to wait. The greater the relative threat, the more likely preemptive actions are to be effective, and, therefore, the greater the justification for acting before the enemy can complete preparations and mount its aggressive attack.

Conceptually, each victim state has a different window of opportunity within which it must act to counter the impending attack. In some cases, the window is wide, extending even to the point of attack itself. In others, it may be much narrower. Unless international law requires the potential victim to simply suffer the attack before responding,[127] the proper standard for evaluating an anticipatory operation must be whether or not it occurred during the last possible window of opportunity. Hence, the appropriate question relates more to the correct timing of the preemptive strike than to the imminence of the attack that animates it.

It is not sufficient to look entirely to the victim state. The likelihood of the pending attack should also determine the appropriateness of forceful response in self-defense. Focusing on this point, Professor Yoram Dinstein has (despite rejecting the "anticipatory" terminology) suggested the admissibility of "interceptive" defense under Article 51.

Interceptive . . . self-defence takes place after the other side has committed itself to an armed attack in an ostensibly irrevocable way. Whereas a preventive strike anticipates an armed attack which is merely "foreseeable" (or even just "conceivable"), an interceptive strike counters an armed attack which is "imminent" and practically "unavoidable."[128]

Anticipatory self-defense most effectively realizes the presumption against violence, the preference for community responses, and the right of a State to survival by combining the two elements. Defense in advance of the attack is legitimate if the potential victim must immediately act to defend itself in a meaningful way and if the potential aggressor has irrevocably committed itself to attack. Without the first requirement, anticipatory self-defense risks missing opportunities to resolve the situation peacefully; without the second, a danger exists of responding to an attack that is speculative at best.

A wide array of computer network attack operations executed to prepare the battle space may meet this standard. By the anticipatory self-defense standard, the right of a state to respond forcefully to them would depend not so much on the nature of the information operation, as on its significance vis-à-vis the coming armed attack. Does the CNA appear merely preparatory or is it more likely an irreversible step in the final chain of events? Placement of a logic bomb in an air defense sector's warning network does not demand an immediate retort. Attempting to corrupt the system as troops are massed along the border and the enemy's air force has just completed a 48-hour stand-down represents a much more serious threat and may well merit an immediate defensive response. How capable is the state of defending itself in the event the attack does come? The logic bomb is only a potential interference with future operations, whereas corruption of the air defense system may require a prompt response lest the opponent be able to destroy the victim State's air force on the ground without warning. Is the CNA the sort of act that logically fits into a near-term attack sequence? Attacking supply and transportation computer networks fits because it would hinder reinforcement

and resupply efforts. So too do attacks on communication systems, as C3 attacks are highly likely immediately preceding any attack.[129] By contrast, attacking defense research facility networks does not fit into a near-term attack sequence because the benefits of most such operations are likely to be reaped long after the computer attack occurs.

Essentially, the right to respond forcefully in self-defense to a computer network attack that does not in and of itself constitute an armed attack arises upon the confluence of three factors:

> 1) The CNA is part of an overall operation culminating in armed attack;
> 2) The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and
> 3) The defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.[130]

Note that it is not the CNA that is actually being defended against, but instead the overall armed attack, complete with its information operation component. Thus, compliance with the requirement that acts in self-defense be proportional is measured against the armed attack, not the CNA.[131] For the same reason, the attack need not be against the facility that launched the CNA or even designed to counter this or other computer network attacks. Again, the armed attack is the normative driver, not the information operation.

The final issue surrounding self-defense is whether Article 51 subsumes the "inherent right" to self-defense, in other words whether a separate and distinct right exists in customary international law. Clearly, a customary law right to self-defense exists, a fact recognized by the ICJ in the Nicaragua case. But is that right only meaningful to states which are not party to the UN Charter (or those which would exercise collective defense to come to their assistance) or does the right exist altogether separately? Is it limited to armed attack, and does it evolve in different directions and at a different pace? This debate has permeated scholarship and practice regarding the law of self-defense for the last five decades.[132] However, in the context of the Charter security scheme, the right clearly appears limited to defense against armed attacks. If a less restrictive customary international law norm would permit responses to situations other than armed attacks, parties to the Charter would still be bound by their treaty obligation. Of course, an operational code regarding defensive responses to CNA which varies from the armed attack standard could develop that is less-restrictive than Article 51. That would not alter the content of the standard, but simply relegate it to the positivist myth system.

IV. Concluding Thoughts on the Appropriate Normative Framework

Computer network attack represents a new tool of coercion in the international arena, one that is fundamentally different from those previously available. Arguably, its distinctiveness merits consideration of a new and unique normative framework to specifically address computer network attack or, more broadly, information operations. However, consensus on the need for such an effort, let alone its substantive content, is unlikely to be achieved at any time in the near future.

Cognizant of this reality, and of the fact that efforts to develop and field computer network attack capability are being pursued vigorously, the essay considers this new

coercive technique within the current prescriptive environment. It suggests an analysis of computer network attack under international law, particularly as framed with the U.N. Charter, that would proceed as follows.

1) Is the technique employed in the CNA a use of armed force? It is if the attack is intended to directly cause physical damage to tangible objects or injury to human beings.
2) If it is not armed force, is the CNA nevertheless a use of force as contemplated in the U.N. Charter? It is if the nature of its consequences track those consequence commonalities which characterize armed force.
3) If the CNA is a use of force (armed or otherwise), is that force applied consistent with Chapter VII, the principle of self-defense, or operational code norms permitting its use in the attendant circumstances?
    a) If so, the operation is likely to be judged legitimate.
    b) If not and the operation constitutes a use of armed force, the CNA will violate Article 2(4), as well as the customary international law prohibition on the use of force.
    c) If not and the operation constitutes a use of force, but not armed force, the CNA will violate Article 2(4).
4) If the CNA does not rise to the level of the use of force, is there another prohibition in international law that would preclude its use? The most likely candidate, albeit not the only one, would be the prohibition on intervening in the affairs of other States.

Assuming a CNA occurs, the appropriateness of a response by armed force may be analyzed in the following manner:

1) If the computer network attack amounts to a use of armed force, then the Security Council may characterize it as an act of aggression or breach of peace and authorize a forceful response under Article 42 of the Charter. To constitute an armed attack, the CNA must be intended to directly cause physical damage to tangible objects or injury to human beings.
2) If the CNA does not constitute an armed attack, the Security Council may nevertheless find it to threaten the peace (the absence of inter-state violence) and authorize a use of force to prevent a subsequent breach of peace. The CNA need not amount to a use of force before the Council may determine that it threatens peace.
3) States, acting individually or collectively, may respond to a CNA amounting to armed attack with the use of force pursuant to Article 51 and the inherent right of self-defense.
4) States, acting individually or collectively, may respond to a CNA not amounting to armed attack, but which is an integral part of an operation intended to culminate in armed attack when:
    a) The acts in self-defense occur during the last possible window of opportunity available to effectively counter the attack; and
    b) The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack.

The indeterminacies in this scheme are the evolution of customary law and the emergence of operational code norms. It is entirely possible that customary law norms restricting the use of CNA beyond Charter levels could emerge. However, any such

process would be incremental. Much more likely is emergence of new operational codes, either enhancing or relaxing existing norms, in response to the exploding possibilities of information operations.

To the extent that such codes reflect the expectations of the politically effective actors on the international scene, policy vectors assume normative valence. The United States, unfortunately, faces a dilemma with regard to an appropriate policy stance vis-à-vis computer network attack. Its technological wherewithal renders it the state most capable of conducting information operations, but also the one most vulnerable, particularly to CNA. The temptation to exploit one's strengths drives much of the serious attention paid by U.S. government agencies, both military and civilian, to offensive information operations. However, as time goes on our relative advantage will inevitably slip as IO know-how diffuses to increasing numbers of states. Moreover, it will prove an attractive asymmetric option to states unable to field forces to the level of the United States and its closest allies.

Given this likely unfolding of events, perhaps the policy approach that best fosters U.S. interests is one advocating a restrictive view of the permissibility of computer network attack. Since the Charter use of force prohibition reflects a fair degree of imprecision in the CNA context, this approach would favor greater inclusivity in gray area applications of the norm. This predilection to restrictions on CNA operations should not be interpreted as a suggestion that the criteria for armed attack be relaxed. On the contrary, maintaining a relatively high threshold for triggering the right to respond to CNA in self-defense, although not enhancing its deterrent effect, serves to maintain constraints on the usually more disruptive act of unilateral resort to armed force. Furthermore, should an information operation be mounted that raises the question of whether an act of armed force has occurred, it would in all likelihood amount to a threat to the peace and thereby seize the Security Council of the matter. This may be faint consolation for the state facing a serious computer network attack, but from a world order perspective it represents the optimal alternative. As Myres McDougal and Federico Feliciano eloquently noted nearly four decades ago,

The overwhelming common interest in basic order, and the exorbitant potential costs of exercise of force by contemporary weapons would appear to counterbalance losses states may occasionally incur from lesser wrongs left inadequately redressed because of deficiencies in available remedial procedures or the limited ability of a poorly organized community to create effective remedies for all wrongs.[133]

Ultimately, of course, it is achievement of world order that best fosters the shared community values underlying the jus ad bellum.

About the Institute

The Institute for Information Technology Applications (IITA) was formed in 1998 to provide a means to research and investigate new applications of information technology. The Institute encourages research in education and applications of the technology to Air Force problems that have a policy, management, or military importance. Research grants enhance professional development of researchers by providing opportunities to work on actual problems and to develop a professional network.

Sponsorship for the Institute is provided by the Secretary of the Air Force for Acquisition, the Air Force Office of Scientific Research, and the Dean of Faculty at the U.S. Air Force Academy. IITA coordinates a multidisciplinary approach to research that incorporates a wide variety of skills with cost-effective methods to achieve significant results. Proposals from the military and academic communities may be submitted at any time since awards are made on a rolling basis. Researchers have access to a highly flexible laboratory with broad bandwidth and diverse computing platforms.

To explore multifaceted topics, the Institute hosts single-theme conferences to encourage debate and discussion on issues facing the academic and military components of the nation. More narrowly focused workshops encourage policy discussion and potential solutions. IITA distributes conference proceedings and other publications nation-wide to those interested or affected by the subject matter.

Endnotes

[1] *See* CHARLES SWETT, STRATEGIC ASSESSMENT: TH INTERNET (July 17, 1995), available at <http://www.fas.org/cp/swett.htm]>. To illustrate the global nature of the phenomenon, consider the number of computers linked to the worldwide net per ten thousand persons for selected countries: Finland, 500+; U.S., 300+; Norway, Australia, New Zealand, Sweden, 200+; Denmark, Switzerland, Canada, Netherlands, Singapore, 100+; United Kingdom, nearly 100. *See* Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Directorate for Information Operations, Presentation at National Defense University (Jan. 1998).

[2] *See Information Security: Computer Attacks at Department of Defense Pose Increasing Risks: Testimony Before the Permanent Sub Comm. on Investigations of the Senate Comm. On Governmental Affairs*, 104th Cong. (1996) (statement of Jack L. Brock, Director, Defense Information and Financial Management Systems Accounting and Information, General Accounting Office)[herinafter Brock]; ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS (GAO/T-AIMD-96-92, May 22, 1996).

[3] *See* Brock, *supra* note 2

[4] On the changing face of war and its relationship to the law of armed conflict, *see generally* Michael Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict, in* THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM 389 (Michael Schmitt & Leslie Green eds., 1998). For more general discussion of the "revolution in military affairs," see WILLIAM S. COHEN, SECRETARY OF DEF., ANN. REP. TO THE PRESIDENT AND CONGRESS, ch. 13 (1998); Dennis M. Drew, *Technology and the American Way of War: Worshipping a False Idol?*, AIR FORCE J. LOGISTICS, Winter 1987, at 21; James R. Fitzsimonds, *The Coming Military Revolution: Opportunities and Risks*, PARAMETERS, Summer 1995, at 30; Dan Gouré, *Is There a Military-Technical Revolution in America's Future?*, WASH. Q., Autumn 1993, at 175; Andrew F. Krepinevich, Jr., *Cavalry to Computer: The Pattern of Military Revolutions, in* STRATEGY AND FORCE PLANNING 582 (Naval War College Faculty ed., 1995); Andrew F. Krepinevich, Jr., *Keeping Pace with the Military-Technical Revolution*, ISSUES IN SCIENCE & TECHNOLOGY, Summer 1994, at 23; Kenneth F. McKenzie, Jr., *Beyond Luddites and Magicians: Examining the MTR*, PARAMETERS, Summer 1995, at 15; Abhi Shelat, *An Empty Revolution: MTR Expectations Fall Short*, HARVARD INTERNATIONAL REVIEW, Summer 1994, at 52.

[5] Bibliographies on information operations are available on-line. *See, e.g., An IW Bibliography* (visited Feb. 24, 1999) <http:// www.infowar.com/RESOURCE/IWBIB1.html-ssi>; Air University, *Information Warfare* (visited Feb. 24, 1999) <http://www.au.af.mil/au/aul/bibs/infowar/if.htm>; Naval War College, *Library Notes* (visited Feb. 24, 1999) <http://www.nwc.navy.mil/library/libinfwf.htm>. For an introduction to the subject, see generally THE INFORMATION AGE: AN ANTHOLOGY ON ITS IMPACT AND CONSEQUENCES (David S. Alberts & Daniel S. Papp eds., 1997); CYBERWAR : SECURITY, STRATEGY, AND CONFLICT IN THE INFORMATION AGE (Alan Campen, ed., 1996); CYBERWAR 2.0: MYTHS, MYSTERIES AND REALITY (Alan Campen & Douglas Dearth eds., 1998); MARTIN C. LIBICKI, THE MESH AND THE NET: SPECULATIONS ON ARMED CONFLICT IN A TIME OF FREE SILICON (1995); MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? (1995); WINN SCHWARTAU, INFORMATION WARFARE: CHAOS ON THE ELECTRONIC SUPERHIGHWAY (1994). A number of these works and others on information warfare are available on-line at the National Defense University's electronic books website. *See National Defense University Press Books On-line* (visited Feb. 24, 1999) <http://www.ndu.edu/inss/books/books.html>

[6] JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS GL-5 (Oct. 9, 1998) [hereinafter JOINT PUB. 3-13].

[7] For surveys on information operations and the law, see generally Office of the Judge Advocate General, Headquarters United States Air Force, A Primer on Legal Issues in Information Warfare (3d ed., 1997); David J. DiCenso, Information Operations: An Act of War? (Oct. 7, 1998) (unpublished report for the Institute of National Security Studies, U.S. Air Force Academy); Charles Dunlap, *The Law of Cyberwar: A Case Study from the Future, in* CYBERWAR 2.0: MYTHS, MYSTERIES AND REALITY (Alan Campen & Douglas Dearth eds., 1998); LAWRENCE GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW (1998); Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272 (1996); Mark R. Shulman, *Discrimination in the Laws of Information Warfare*, 37 COLUM. J. TRANS. L. 939 (1999).

[8] Although efforts to affect an opponent's information base and protect one's own have characterized warfare throughout history, it is only in the last decade that IO has been recognized as a distinct form of warfare meriting its own separate doctrine, policy, and tactics.

[9] JOINT PUB. 3-13, *supra* note 6, at GL-7. For the IO policy of U.S. forces, see generally INFORMATION OPERATIONS, U.S. DEP'T OF DEF. DIRECTIVE (DODD) S-3600.1 (Dec. 9, 1996); JOINT INFORMATION OPERATIONS POLICY, CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION (CJCSI) 3210.01A (Jan. 1996). Other official IO-related guidance includes: DEFENSIVE INFORMATION WARFARE OPERATIONS IMPLEMENTATION, CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION (CJCSI) 6510.01 (Aug. 22, 1997); JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.1, JOINT DOCTRINE FOR

COMMAND AND CONTROL WARFARE, (Feb. 7, 1996) [hereinafter JOINT PUB. 3-13.1]; JOINT CHIEFS OF STAFF, JOINT PUB. 3-53, DOCTRINE FOR JOINT PSYCHOLOGICAL OPERATIONS (July 10, 1996) [hereinafter JOINT PUB. 3-53]; JOINT CHIEFS OF STAFF, JOINT PUB. 3-58, JOINT DOCTRINE FOR MILITARY DECEPTION (May 31, 1996) [hereinafter JOINT PUB. 3-58]; U.S. DEP'T OF THE NAVY, CHIEF OF NAVAL OPERATIONS INSTRUCTION 3430.26, IMPLEMENTING INSTRUCTION FOR INFORMATION WARFARE COMMAND AND CONTROL (Jan. 18, 1995); U.S. DEP'T OF THE NAVY, NAVAL DOCTRINE PUBLICATION 6, NAVAL COMMAND AND CONTROL (May 19, 1995); U.S. DEP'T OF THE AIR FORCE, AIR FORCE DOCTRINE DOCUMENT 2-5, INFORMATION OPERATIONS (Aug 5, 1998); U.S. DEP'T OF THE ARMY, U.S. ARMY FIELD MANUAL 100-6, INFORMATION OPERATIONS (Aug. 27, 1996); U.S. DEP'T OF THE MARINES, MARINE CORPS ORDER 3430.1, POLICY FOR INFORMATION OPERATIONS (May 19, 1997). *See also* U.S. DEP'T OF THE AIR FORCE, THE CORNERSTONES OF INFORMATION WARFARE (1995). Many U.S. military publications are available on-line. *See Joint Electronic Library* (visited Feb. 24, 1999) <http://www.dtic.mil/doctrine/jel/>.

[10] JOINT PUB. 3-13, *supra* note 6, at GL-7 (emphasis added).

[11] *See* U.S. DEP'T OF DEFENSE, JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 387 (March 23, 1994, as amended through June 10, 1998), *available at DODD Dictionary of Military Terms* (visited Feb. 24, 1999) <http://www.dtic.mil/doctrine/jel/doddict/> [hereinafter JOINT PUB. 1-02]. The key distinguishing characteristic of sabotage is its design to interfere with the national defense. Thus, an attack on the banking system would not constitute sabotage, but one on a factory manufacturing military equipment would.

[12] *See id.* at 217. Information operations must also be distinguished from command and control warfare (C2W), a form of IO with the specific purpose of influencing, degrading, or destroying an opponent's ability to direct its forces. On C2W, see JOINT PUB. 3-13.1, *supra* note 9.

[13] Defensive IO "integrate[s] and coordinate[s] policies and procedures, operations, personnel, and technology to protect and defend information and information systems." Activities that support defensive IO include "information assurance (IA), OPSEC [operations security], physical security, counterdeception, counterpropoganda, counterintelligence (CI), EW [electronic warfare], and SIO [special information operations]." JOINT PUB. 3-13, *supra* note 6, at I-10. Each of these terms is defined in the Glossary to JOINT PUB. 3-13, *supra* note 6. Offensive IO, by contrast, is intended to "affect adversary decision makers and achieve or promote specific objectives." *Id.* at I-10.

[14] "Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission." JOINT PUB. 1-02, *supra* note 11, at 281.

[15] "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 . . . is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives." *Id.* at 358.

[16] "Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy." *Id.* at 151.

[17] "Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process." JOINT PUB. 3-13, *supra* note 6, at GL-10.

[18] Strategic objectives are those at the national or multinational level. Operational objectives lie at the level of major military campaigns or of a military theater of operations. Tactical objectives arise at the individual battle or engagement level.

[19] In fact, IO has been characterized as possibly having its "greatest impact in peace and the initial stages of crisis." JOINT CHIEFS OF STAFF, INFORMATION WARFARE: A STRATEGY FOR PEACE . . . THE DECISIVE EDGE IN WAR 5 (n.d.). This is because many, if not most, of its effects are other than physical destruction. Indeed, according to the JCS, "IW [*sic*] can make an important contribution to defusing crises; reducing the period of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ forces in a combat situation." *Id.*

[20] *See* ROGER C. MOLANDER ET AL., STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR 66 (1996).

[21] *See* Kanuck, *supra* note 7, at 289.

[22] *See* Molander, *supra* note 20, at 74.

[23] *See* PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES A-48 (Oct 1997).

[24] *See id.* at A-46.

[25] *See* TED UCHIDA, SCHOOL OF ADVANCED MILITARY STUDIES, U.S. ARMY COMMAND AND GENERAL STAFF COLLEGE, BUILDING A BASIS FOR INFORMATION WARFARE RULES OF ENGAGEMENT 8 (1997). In order to test computer security, DISA periodically uses typical "hacker-tools" to attack DOD computers. During a test of over twenty-six thousand unclassified computers in 1995, only 2% of the intrusions were detected, and of those only 5% were properly reported to the appropriate authorities. *See* DEFENSE SCIENCE BOARD TASK FORCE, INFORMATION WARFARE: DEFENSE (IW-D) 2-15 (Nov. 1996). In another study looking at the results of fifty-nine assessments involving 37,518 computers, 3.6% had

easily exploitable "back-doors," 65% could be penetrated once the intruder was inside the network, 96% of professionally conducted penetrations go undetected by systems administrators and users, and 73% of detected penetrations were not reported. *See* Paul A. Strassmann, Information Terrorism: The Ultimate Infosec Challenge, Briefing at National Defense University (Jan. 5, 1998).

[26] *See* OFFICE OF SCIENCE AND TECHNOLOGY POLICY, EXECUTIVE OFFICE OF THE PRESIDENT, CYBERNATION: THE AMERICAN INFRASTRUCTURE IN THE INFORMATION AGE (Apr. 1997).

[27] *See id.*

[28] *Id.* The Defense Science Board Task Force also noted this point.

> Our Task Force had many enlightening discussions about the potential for effects to cascade through one infrastructure (such as the phone system) into other infrastructures. This example is particularly important because most of our other infrastructures ride on the phone system. No one seems to know quite how, where, or when effects actually would cascade; nor what the total impact would be.

DEFENSE SCIENCE BOARD TASK FORCE, *supra* note 25, at 2-14

[29] The President's Commission on Critical Infrastructure Protection focused on the existence of infrastructures and the vulnerabilities they represent.

> Life is good in America because things work . . . We are able to assume that things will work because our infrastructures are highly developed and highly effective . . . By *infrastructure* we mean more than just a collection of individual companies engaged in related activities; we mean a network of independent, mostly privately owned, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.

It noted the criticality of certain aspects of the infrastructure.

- Transportation . . . moves goods and people within and beyond our borders, and makes it possible for the United States to play a leading role in the global economy.
- Oil and gas production and storage . . . infrastructure fuels transportation services, manufacturing operations, and home utilities.
- The water supply infrastructure assures steady flow of water for agriculture, industry (including various manufacturing processes, power generation, and cooling), business, fire fighting, and our homes.
- Government services . . . consists of federal, state, and local agencies that provide essential services to the public.
- Banking & finance . . . manages trillions of dollars, from deposit of our individual paycheck to the transfer of huge amounts in support of major global enterprises.
- Electrical power infrastructure . . . [includes] generation, transmission, and distribution systems that are essential to all other infrastructures and every aspect of our economy.
- Telecommunications [have] . . . been revolutionized by advances in information technology in the past two decades to form an information and communications infrastructure, consisting of the Public Telecommunications Network (PTN), the Internet, and the many millions of computers in home, commercial, academic, and government use . . . connected to one another . . . Networking is essential to a service economy as well as to competitive manufacturing and efficient delivery of raw materials and finished goods. The information and communications infrastructure is basic to responsive emergency services. It is the backbone of our military command and control system. And it is becoming the core of our educational system.

PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 23, at 3-4.

[30] Arsenio T. Gumahad II, *The Profession of Arms in the Information Age*, JOINT FORCE Q., Spring 1997, at 14, 18, citing WIRED MAGAZINE, July-Aug. 1993. An interesting IO scenario was used during a war game at National Defense University. Set in the year 2000, it involved an OPEC meeting that goes awry when Saudi Arabia opposes Iranian demands for an oil production cutback in order to drive prices up. Iran mobilizes and conducts several attacks on Saudi warships. It also begins to conduct information warfare operations to destabilize the Saudi regime and keep the United States and United Kingdom out of the fray. A Saudi refinery is destroyed when computer malfunctions in its control mechanisms cause a fire; a "logic bomb" placed in the computer system running U.S. railways causes a passenger train to derail; computer "worms" begin to corrupt the U.S. military's classified deployment database, and a "sniffer" disrupts fund transfers in the Bank of England. *See* Steve Lohr, *Ready. Aim. Zap*; *National Security Experts Plan for Wars Whose Targets and Weapons are all Digital*, N.Y. TIMES, Sept. 30, 1996, at D-1.

[31] On asymmetry, see generally Schmitt, *supra* note 4.

[32] Planning Considerations for Defensive Information Warfare, Task Order 90-SAIC-019, Dec. 16, 1993 (*prepared for* The Defense Information Systems Agency, Joint Interoperability and Engineering Organization, and Center for Information Systems Security) (citing Robert D. Steele, War and Peace in the Age of Information, Superintendent's Guest Lecture, Naval Postgraduate School (August 1993)) [hereinafter Planning Considerations].

[33] *See* Planning Considerations, *supra* note 32, at 17.

[34] *See* JANE'S ALL THE WORLD'S AIRCRAFT 676 (Paul Jackson et al. eds., 1997-98).

[35] *See* PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 23, at 9. Moreover, there will be approximately 1,300,000 "telecommunications systems control software specialists with tools and know how to disrupt or take down the public telecommunications network." *Id.*

[36] *See* Brock, *supra* note 2, at 5.

[37] *See* HAI LUNG & CHANG FENG, CHINESE MILITARY STUDIES INFORMATION WARFARE, (Hong Kong PTS Msg 210225Z Feb. 96, Subj: PLA Undertakes Study of Information Warfare) (Publications Translations Section, U.S. Consulate General, Hong Kong trans.).According to the report, preparations are underway for the establishment of an Information Warfare Institute, a non-governmental entity that will be responsible for "strategic planning . . ., theoretical studies, and technological development. Its aim is to enable high-technology advances from the nonmilitary sector to be applied to the military sector under the guidance of military theory." *Id.* Russia is also interested in enhancing IO capabilities. *See, e.g.,* Mary C. FitzGerald, *Russian Views on Electronic and Information Warfare, in* NATIONAL DEFENSE UNIVERSITY, PROCEEDINGS OF THE THIRD INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM: PARTNERS FOR THE 21ST CENTURY 126 (1997).

[38] *See* Mark Walsh, *U.S. Military Expands Information Warfare Defense*, DEF. NEWS, Apr. 28-May 4, 1997, at 25; Lohr, *supra* note 30, at D4.

[39] OFFICE OF THE PRESS SECRETARY, THE WHITE HOUSE, A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY (May 17, 1997) (visited Feb. 23, 1999) <http://www1.whitehouse.gov/WH/html/library-plain.html>.

[40] JOINT CHIEFS OF STAFF, NATIONAL MILITARY STRATEGY: SHAPE, RESPOND, PREPARE NOW, A MILITARY STRATEGY FOR A NEW ERA (1997) (visited Feb. 23, 1999) <http://www.dtic.mil/jcs/nms>.

[41] U.N. CHARTER art. 2, para 4.

[42] *See id.* art. 1, para 1.

[43] For instance, the General Assembly, in its resolution regarding the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, has provided that,

> Every State has a duty to refrain in its international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations. Such a threat or use of force constitutes a violation of international law and the Charter of the United Nations and shall never be employed as a means of settling international issues.

G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N. Doc. A/8082 (1970), *reprinted in* KEY RESOLUTIONS OF THE UNITED NATIONS GENERAL ASSEMBLY, 1946-1996, at 3 (Dietrich Rauschning et al. eds., 1997) [hereinafter Declaration on Friendly Relations]. The resolution was adopted by acclamation.

[44] The analysis which follows will address uses of force, but applies equally to *threats* to use force. In other words, to the extent that CNA constitutes a use of force, the threat to commit such an attack will also be prohibited. On threats, see Romana Sadurska, *Threats of Force*, 82 AM. J. INT'L L. 239 (1988).

[45] Originally, the draft of the Charter did not contain the terms territorial integrity or political independence, and the proposal for their inclusion was controversial. However, the travaux make it clear that the "other manner" language filled any possible voids in coverage. *See* Doc. 1123, I/8, 6 U.N.C.I.O Docs. 65 (1945); Doc 784, I/1/27, 6 U.N.C.I.O. Docs. 336 (1945); Doc. 885, I/1/34, 6 U.N.C.I.O. Docs. 387 (1945). *See also* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 265-69 (1963) [hereinafter BROWNLIE, USE OF FORCE]. For a brief discussion of this issue in the context of information operations, see James N. Bond, Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4), at 55-56 (June 14, 1996) (Advanced Research Project, United States Naval War College).

[46] *See, e.g.,* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 86 (2d ed. 1994); Josef Mrazek, *Prohibition of the Use and Threat of Force: Self-Defence and Self-Help in International Law*, 27 CAN. Y.B. INT'L L. 81, 90 (1989); Albrecht Randelzhofer, *Article 2(4), in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 106, 117-18 (Bruno Simma et al. eds., 1995).

[47] Unfortunately, this approach occasionally leads to tortuous efforts to justify operations, such as those in response to terrorist attacks, in Charter (usually self-defense) terms. A classic example would be the 1986 raid (Operation El Dorado Canyon) on Libya by U.S. aircraft in response to the terrorist bombing intended to kill U.S. servicemen at a disco in Berlin. On the operation and its justification, see *President's Address to the Nation, Apr. 14, 1986, reprinted in U.S. Exercises Right of Self-defense Against Libyan Terrorism*, DEP'T ST. BULL., at 1 (June 1986). Much attention

has been paid to the fact that Libya was planning attacks on up to thirty U.S. diplomatic facilities worldwide. *See Joint News Conference by Secretary Schultz and Secretary Weinberger, April 14, 1986, reprinted in U.S. Exercises Right of Self-defense Against Libyan Terrorism*, *supra*, at 3 (June 1986).

[48] W. Michael Reisman, *Criteria for the Lawful Use of Force in International Law*, 10 YALE J. INT'L L. 279, 281 (1985) [hereinafter Reisman, *Criteria*]. *See also* W. Michael Reisman, *Article 2(4):The Use of Force in Contemporary International Law*, 78-79 AM. SOC. INT'L L. PROC. 74, 79-84 (1984-85); W. Michael Reisman, *War Powers: The Operational Code of Competence*, 83 AM. J. INT'L L. 777 (1989).

[49] *See* Reisman, *Criteria*, *supra* note 48, at 282.

[50] For an interesting projection of factors likely to affect the use of force in the future, see Anthony D'Amato, *Megatrends in the Use of Force*, *in* THE LAW OF ARMED CONFLICT, *supra* note 4, at 1.

[51] Vienna Convention on the Law of Treaties, May 23, 1969, art. 31(1), 1155 U.N.T.S. 331 (1969). This point was reiterated by the International Court of Justice in *The Competence of the General Assembly for the Admission of a State to the United Nations* case. In that case, the ICJ noted that "the first duty of a tribunal which is called upon to interpret and apply the provisions of a treaty is to endeavor to give effect to them in their natural and ordinary meaning in the context in which they occur." General List No. 9, 1950 I.C.J. 4, 8 (Mar. 3) (advisory opinion).

[52] *See* Randelzhofer, *supra* note 46, at 112; Hans Wehberg, "L'Interdiction du Recours á la Force: Le Principe et les Problèmes qui se Posent," 78 R.C.A.D.I. 1, 69 (1951).

[53] Vienna Convention, *supra* note 51, art. 31(2).

[54] *Id.* arts. 41, 46.

[55] U.N. CHARTER art. 111.

[56] Vienna Convention, *supra* note 51, art. 32. ("Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31: (a) Leaves the meaning ambiguous or obscure; or (b) Leads to a result which is manifestly absurd or unreasonable").

[57] "Legislative history," specifically the record of negotiations leading to final adoption of the Convention.

[58] *See* Doc. 784, I/1/27, 6 U.N.C.I.O. Docs. 331, 334, 609 (1945). Originally, the Dumbarton Oaks Proposal for the prohibition read as follows: "All members of the Organization shall refrain from the threat or use of force in any manner inconsistent with the purposes of the Organization." Doc. 1123 I/8, 6 U.N.C.I.O. Docs. 65, 68 (1945).

[59] *See* Doc. 2, G/7 (e)(4), 3 U.N.C.I.O. Docs. 251, 253-54 (1945).

[60] *See, e.g.*, Inter-American Treaty of Reciprocal Assistance, Sept. 2, 1947, art. 1, T.I.A.S. No. 1838, 21 U.N.T.S. 77: ". . . undertake in their international relations not to resort to the threat or the use of force in any manner inconsistent with the provisions of the Charter of the United Nations or of this Treaty." *See also* Pact of the League of Arab States, March 22, 1945, art. 5, 70 U.N.T.S. 238, which only speaks of force; "Any resort to force in order to resolve disputes arising between two or more member States of the League is prohibited." This instrument was drafted contemporaneously with the U.N. Charter.

[61] Charter of the Organization of American States, Apr. 30, 1948, T.I.A.S. No. 2361, 119 U.N.T.S. 3.

> Article 18: No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic, and cultural elements.

Article 19: No State may use or encourage the use of coercive measures of an economic or political character in order to force the sovereign will of another State and obtain from it advantages of any kind.

[62] Recall that Brazil had proposed that Article 2(4) of the U.N. Charter encompass economic coercion. *See supra* text accompanying note 58.

[63] *See* Declaration on Friendly Relations, *supra* note 43, prin. 1, annex (The General Assembly "[s]olemnly proclaims the following Principles: 1. The Principle that States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations.").

[64] U.N. GAOR Special Comm. On Friendly Relations, 24th Sess., 114th mtg., U.N. Doc. A/AC.125/SR.114 (1970). *See also Report of the Special Comm. on Friendly Relations*, U.N. GAOR, 24th Sess., Supp. No. 19, at 12, U.N. Doc. A/7619 (1969); Derek W. Bowett, *Economic Coercion and Reprisals by States*, 13 VA. J. INT'L L. 1 (1972)

[65] *See, e.g.*, "[a] war of aggression," "irregular forces or bands," "acts of civil strife or terrorist acts," "military occupation," "disarmament," etc. Declaration on Friendly Relations, *supra* note 43, prin. 1, annex.

[66] *Id.* For example, "[n]o State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. *Id.*

[67] G.A. Res. 42/22, U.N. GAOR, 42d Sess., 73d plen. mtg., Agenda Item 131, annex, art. I ¶ 7-8 (1988), *reprinted in* KEY RESOLUTIONS, *supra* note 43, at 7.

[68] As to both declarations, recall that by Article 31(3) of the Vienna Convention subsequent agreement regarding interpretation of a Treaty is an appropriate interpretive consideration. *See* Vienna Convention, *supra* note 51, art. 31(3).

[69] On economic sanctions, see Paul Szasz, *The Law of Economic Sanctions*, *in* THE LAW OF ARMED CONFLICT, *supra* note 4, at 455.

[70] This is not to say that international law scholars missed the distinction; it is only to say that it has attained particular significance in the last decade. For instance, Hans Kelsen noted:

> There are two kinds of force not exercised by use of arms: (1) an action of a state directed against another state which constitutes a violation of international law but which is not performed by use of arms; (2) a reprisal which does not involve the use of armed force. Article 2, paragraph 4, refers to the "use of force." It therefore prohibits both kinds of force. Hence, not only is the use of force prohibited but any action of a member state illegal under general international law which is directed against another state is prohibited by the Charter, and the member states are forbidden to resort not only to war but also to reprisals.

HANS KELSEN, COLLECTIVE SECURITY UNDER INTERNATIONAL LAW 57 n.5 (49 Naval War College International Law Studies 1954, 1956). Ian Brownlie disagrees with this assessment, arguing that "there is no evidence . . . that it bears the meaning suggested by Kelsen." BROWNLIE, USE OF FORCE, *supra* note 45, at 362.

[71] Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 4,119, (June 27). Note that the ICJ was not actually applying Article 2(4) *qua* 2(4) because application of the Charter was barred by the U.S. acceptance of jurisdiction (pursuant to Article 36(2) of the Court's Statute) only on the condition that all States involved in the case be party to any multilateral treaty used by the Court to adjudicate the issue. Therefore, the Court applied the customary international law prohibition on the resort to force

[72] For a discussion of force as extending beyond armed force, see Jordan J. Paust & Albert P. Blaustein, *The Arab Oil Weapon: A Threat to International Peace*, 68 AM. J. INT'L L. 410 (1974).

[73] On the appropriateness of applying the economic instrument, see Clinton E. Cameron, *Developing a Standard for Politically Related State Economic Action*, 13 MICH. J. INT'L L. 218 (1991).

[74] These aims derive from those expressed in the Preamble to the U.N. Charter:

> [T]o save succeeding generations from the scourge of war, which twice in our life-time has brought untold sorrow to mankind, and to reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small, and to establish conditions under which justice and respect for the obligations arising from treaties and other sources of international law can be maintained, and to promote social progress and better standards of life in larger freedom.

U.N. CHARTER preamble, art. X, para. X. The final aim was perceptively articulated in W. Michael Reisman, *Allocating Competences to Use Coercion in the Post-Cold War World: Practices, Conditions, and Prospects*, *in* LAW AND FORCE IN THE NEW INTERNATIONAL ORDER 26, 45 (Lori Fisler Damrosch & David J. Scheffer eds., 1991). To a very great extent, these shared values overlap.

[75] Of course, the aims are perhaps at greater risk from internal sources, but Westphalian state-centrism, with its emphasis on the principle of sovereignty, has held back the progress of international law in responding to internal threats. Fortunately, the effort to limit inter-state conflict usually advances community-wide aspirations without imperiling the internal autonomy that sovereignty cherishes.

[76] U.N. CHARTER art. 1.

[77] Moreover, a purely consequence-based standard would risk falling prey to dissonant (e.g., cultural) valuation paradigms. On the subject of valuation paradigms, see Michael N. Schmitt, *War and the Environment: Fault Lines in the Prescriptive Landscape*, ARCHIV DES VÖLKERRECHTS (1999) (forthcoming).

[78] U.N. CHARTER art. 41.

[79] *See* BROWNLIE, USE OF FORCE, *supra* note 45, at 362.

[80] On non-lethal weapons, see James C. Duncan, *A Primer on the Employment of Non-Lethal Weapons*, 45 NAVAL L. REV. 1 (1998).

[81] Arguably, *responsibility* is a seventh commonality. Armed coercion is the exclusive province of states; only they may generally engage in uses of force across borders, and in most cases only they have the ability to do so with any meaningful impact. By contrast, non-governmental entities are often capable of engaging in other forms of coercion (propaganda, boycotts, etc.). Therefore, with armed coercion the likelihood of blurring the relative responsibility of the State, a traditional object of international prescription, and private entities, usually only the object of international administration, narrows. In sum, the consequences of armed coercion are more susceptible to being charged to the State actor than in the case of other forms of coercion. However, this is an issue of assessing State responsibility, not lawfulness. It is a practical challenge, not a normative one.

[82] For summaries of applicable domestic law, see JOINT CHIEFS OF STAFF, INFORMATION ASSURANCE: LEGAL, REGULATORY, POLICY AND ORGANIZATION CONSIDERATIONS (3d ed. 1997), § 4; Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL L. REV. 57, 64-75 (1998). As to responsibility (*see supra* note 78 and accompanying text), in the macro sense it will be difficult to assess because most computer network attacks can be conducted by non-governmental individuals with access to the requisite hard and software; it requires no special infrastructure available only to a government. However, though this factor would augur against characterizing computer network attack in the abstract as a use of force, because it is technologically-dependent, technological means may be able to reliably ascertain the source of the attack as a specific sate or agent thereof. To the extent this is true of a particular method of attack, it increases the appropriateness of labeling it a use of force.

[83] Consequences should not be confused with motivation (justification). The operational code operates based primarily on the latter; it looks to the rationale for the use of force to justify it, not what its consequences are.

[84] Proportionality is a customary international law principle, codified in 1977 Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, arts. 51.5(b) &57.2(iii), *reprinted in* 3 HAROLD S. LEVIE, PROTECTION OF WAR VICTIMS: PROTOCOL 1 TO THE 1949 GENEVA CONVENTIONS 174, 337 (1980). [hereinafter ADDITIONAL PROTOCOL I]. It is defined as "[t]he principle that seeks to limit damage caused by military operations by requiring that the effect of the means and methods of warfare used must not be disproportionate to the military advantage sought." PIETRO VERRI, DICTIONARY OF THE INTERNATIONAL LAW OF ARMED CONFLICT 90 (Edward Markee & Susan Mutti trans., 1992).

[85] Additional Protocol I, *supra* note 84, arts. 54, 55 & 56.

[86] Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, Dec. 10, 1976, art. I. para. 1, 31 U.S.T.S. 333, 1108 U.N.T.S. 151, 16 I.L.M. 88, 91 (1977).

[87] Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131, U.N. GAOR,20th Sess., Supp. No. 14, at 12, U.N. Doc. A/6220 (1965), *reprinted in* KEY RESOLUTIONS, *supra* note 43, at 26.

[88] For example, regarding international telecommunications law see International Telecommunication Convention (with Annexes, Final Protocol, Additional Protocols, Resolutions, Recommendations and Opinions), Oct. 25, 1973, 28 U.S.T. 2495, 1209 U.N.T.S. 32; International Telecommunication Convention, Nov. 6, 1982, S. TREATY DOC. NO. 99-6.

[89] *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 631-32 (4th ed. 1990).

[90] MALCOLM N. SHAW, INTERNATIONAL LAW 659 (4th ed. 1997). The comment is made with particular regard to subsequent practice. Professor Shaw cites, as support for his proposition, Reparations for Injuries Suffered in the Service of the United Nations, 1949 I.C.J. 174 (Apr. 11); Competence of the General Assembly for the Admission of a State to the United Nations, 1950 I.C.J. 4 (Mar. 3); Certain Expenses of the U.N., 1962 I.C.J. 151 (July 20); Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) Notwithstanding Security Council Resolution 276 (1970), 1971 I.C.J. 16 (June 21)

[91] The obvious danger, though, is that the international community will not react, possibly because the actor is a member of the P-5 and vetoes any action. This would encourage states to respond unilaterally at lower levels of force.

[92] *See* Statute of the International Court of Justice, June 26, 1945, art. 38.1(b), 832 U.S.T.S. 993, 1978 Y.B.U.N. 1197. Customary law is a "general practice accepted as law." *Id*.

[93] Belief that compliance with the practice is out of a sense of legal obligation.

[94] *See* North Sea Continental Shelf (F.R.G. v. Den.; F.R.G. v. Neth.), 1969 I.C.J. 3, 44 (Feb. 20).

[95] On the issue of the customary nature of the prohibition, see 1986 I.C.J. 4, 98-101, 147.

[96] *Id.* at 100. The Court did not actually catalogue state practice; instead, it merely noted that state conduct was generally consistent with the rule. Randelzhofer labels this line of argument "highly disputable." Randelzhofer, *supra* note 46, at 126.

[97] The Court cited the unanimous adoption in 1970 of the Declaration on Friendly Relations, *supra* note 43. *See* 1968 I.C.J. 4, 100. Recall that the Declaration reiterated the language of Article 2(4). For criticism of this approach, see Anthony D'Amato, *Trashing Customary International Law*, 81 AM. J. INT'L L. 101 (1987). On the relationship between the Charter and the Declaration, see F.L. Kirgis, *Custom on a Sliding Scale*, 81 AM. J. INT'L L. 146, 147 (1987).

[98] *See* BROWNLIE, USE OF FORCE, *supra* note 45, at 113; Dinstein, *supra* note 46, at 93; PETER MALANCZUK, AKEHURST'S MODERN INTRODUCTION TO INTERNATIONAL LAW 311 (7th rev. ed. 1997).

[99] 1968 I.C.J. 4, 96-97.

[100] *See supra* text accompanying notes 77-80.

[101] In the Commission's commentary on the draft articles of the Law of Treaties (Vienna Convention), the Charter's prohibition of the use of force was cited as "a conspicuous example" of jus cogens. *See* Report of the International Law Commission, 18th Sess., 1966 (II) I.L.C.Y.B. 247. When such peremptory norms emerge, any existing treaty in conflict with them become void and terminate. *See* Vienna Convention, *supra* note 51, art. 53.

[102] *See* 1968 I.C.J. 4, 100.

[103] Vienna Convention, *supra* note 51, art. 53.

[104] 1968 I.C.J. 4, para. 202.

[105] Declaration on Inadmissibility of Intervention, *supra* note 87.

> 1. [N]o State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned.
>
> 2. No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind . . . .
>
> 5. Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State.

Id. at 26. Note that although the United States voted in favor of the resolution, it stated that the resolution was "only a statement of political intention and not a formulation of law." U.N. GAOR, 20th Sess. at 436, U.N. Doc. A/C.1/SR.1423. That said, the Declaration on Friendly Relations purports to articulate basic principles of international law, including that of non-intervention. *See* Declaration on Friendly Relations, *supra* note 43. The United States offered no statement challenging that characterization.

[106] *See* Declaration on Friendly Relations, *supra* note 43.

[107] In the Corfu Channel case, the International Court of Justice held, in response to the United Kingdom's argument that it had entered Albanian waters to seize evidence, that, "[i]ntervention 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." The Corfu Channel Case (U.K. v. Alb.),1949 I.C.J. 4, 35 (Apr. 9).

[108] U.N. CHARTER art. 39. For an excellent commentary on the article, see Jochen Frowein, *Article 39, in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 46, at 605.

[109] U.N. CHARTER art. 41 (According to the article, "[t]hese may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.").

[110] U.N. CHARTER art. 42 ("Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.").

[111] When engaged as combatants, U.N. forces follow the Guidelines for U.N. Forces Regarding Respect for International Law (FAD/TM, May 1996, 005797) (on file with Author). On the applicability of the law of armed conflict to peace operations, see Umesh Palwankar, *Applicability of International Humanitarian Law to United Nations Peace-Keeping Forces*, INT'L REV. RED CROSS, May-June 1993, at 227; Memorandum of the ICRC to the Governments of the States Party to the Geneva Conventions and Members of the United Nations on the Applicability of the Geneva Conventions by the Military Units Placed at the Disposal of the United Nations, Nov. 10, 1961, *reprinted in* INT'L REV. RED CROSS, Dec. 1961, at 490.

[112]Proposals were made by Bolivia [*see* Doc. 2 G/14 (r), 3 U.N.C.I.O. Docs. 585 (1945)], the Philippines [*see* Doc. 2 G/14 (k), 3 U.N.C.I.O Docs. 538 (1945)], and Czechoslovakia [*see* Doc. 2 G/14 (b), 3 U.N.C.I.O Docs. 469 (1945)]. The Bolivian proposal was supported by Columbia, Egypt, Ethiopia, Guatemala, Honduras, Iran, Mexico, New Zealand, and Uruguay. *See* Doc. 442 III/3/20, 12 U.N.C.I.O. Docs. 341 (1945). The U.S. and U.K. opposed a delineation of acts of aggression on the ground that doing so might force responses by the Security Council that would not otherwise be justified. *Id.* at 341-42. Ultimately, the proposal for defining aggression was rejected by a 22-12 vote. *See* Doc. 502/3/22, 12 U.N.C.I.O. Docs. 349 (1945).

[113] Definition of Aggression, G.A. Res. 3314 (XXIX), art. 1, U.N. GAOR, 29th Sess., Supp. No. 31, at 142, U.N. Doc. A/9631 (1975), 13 I.L.M. 710 (1974), *reprinted in* KEY RESOLUTIONS, *supra* note 43, at 13. Judge Schwebel of the United States addressed the significance of the resolution in his dissent in the *Nicaragua* case.

> The significance of the Definition of Aggression—or of any definition of aggression—should not be magnified. It is not a treaty. It is a resolution of the General Assembly which rightly recognizes the supervening force of the United Nations Charter and the supervening authority in matters of aggression of the Security Council. The Definition has its conditions, its flaws, its ambiguities and uncertainties. It is open ended. Any definition of aggression must be, because aggression can only be ultimately defined and found in the particular case in light of its particular facts. At the same time, the Definition of Aggression is not a resolution of the General Assembly which purports to declare principles of customary international law not regulated by the United Nations Charter . . . . This resolution rather is an interpretation by the General Assembly of the meaning of the provisions of the United Nations Charter governing the use of force . . . .

1968 I.C.J. 4, 345.

[114] In Article 3, the General Assembly offered examples of aggression:

> Any of the following acts, regardless of a declaration of war, shall be subject to and in accordance with the provisions of Article 2, qualify as an act of aggression:
>
> a) The invasion or attack by the armed forces of a State of the territory of another state . . . or any annexation . . . ;
>
> b) Bombardment . . . against the territory of another State or the use of any weapons by a State against the territory of another State;
>
> c) . . . blockade . . . ;
>
> d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
>
> e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond term of the agreement;
>
> f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
>
> g) 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 the acts listed above, or its substantial involvement therein.

Definition of Aggression, *supra* note 43, art. 3.

[115] U.N. CHARTER art. 1, para. 2.

[116] *See* Frowein, *supra* note 108, at 612.

[117] *See* S.C. Res. 713, U.N. SCOR, 3009th mtg., U.N. Doc. S/RES/713 (1991). This resolution, and all other Security Council Resolutions are available online at <http://www.un.org/Docs/sc.htm>.

[118] *See* S.C. Res. 733, U.N. SCOR, 3039th mtg., U.N. Doc. S/RES/733 (1992).

[119] *See* S.C. Res. 788, U.N. SCOR, 3138th mtg., U.N. Doc. S/RES/788 (1992).

[120] *See* S.C. Res. 748, U.N. SCOR, 3063rd mtg., U.N. Doc. S/RES/748 (1992). Until the demise of the Cold War, the Council, due to the existence of off-setting bloc vetoes, proved impotent in responding to threats to the peace. In only one case (Rhodesia) did it find a threat to the peace and authorize forceful measures in response. In Security Council Resolution 221, the Council authorized the United Kingdom to deny ships carrying oil destined for Rhodesia access, by force if necessary, to the Port of Beira in Mozambique. *See* S.C. Res. 221, U.N. SCOR, 1277th mtg., U.N. Doc. S/RES/221 (1966). The impotence of the Security Council led the General Assembly to adopt the Uniting for Peace Resolution in 1950. It provides that:

> [I]f the Security Council, because of the lack of unanimity of the permanent members, fails to exercise its primary responsibility for the maintenance of international peace and security in any case where there appears to be a threat to the peace, breach of the peace or act of aggression, the General Assembly shall consider the matter immediately with a view to making appropriate recommendation to Members for collective measures, including . . . the use of armed force.

G.A. Res. 377(V), para. 1, 1950 U.N.Y.B. 193-95. *See* S.C. Res. 748, U.N. SCOR, 3063rd mtg., U.N. Doc. S/RES/748 (1992). Until the demise of the Cold War, the Council, due to the existence of off-setting bloc vetoes, proved impotent in responding to threats to the peace. In only one case (Rhodesia) did it find a threat to the peace and authorize forceful measures in response. In Security Council Resolution 221, the Council authorized the United Kingdom to deny ships carrying oil destined for Rhodesia access, by force if necessary, to the Port of Beira in Mozambique. *See* S.C. Res. 221, U.N. SCOR, 1277th mtg., U.N. Doc. S/RES/221 (1966). The impotence of the Security Council led the General Assembly to adopt the Uniting for Peace Resolution in 1950. It provides that:

> [I]f the Security Council, because of the lack of unanimity of the permanent members, fails to exercise its primary responsibility for the maintenance of international peace and security in any case where there appears to be a threat to the peace, breach of the peace or act of aggression, the General Assembly shall consider the matter immediately with a view to making appropriate recommendation to Members for collective measures, including . . . the use of armed force.

G.A. Res. 377(V), para. 1, 1950 U.N.Y.B. 193-95.

[121] U.N. CHARTER art. 51. For an excellent survey of the article, see Albrecht Randelzhofer, *Article 51, in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 46, at 106.

[122] The French text of the Charter uses the term "*agression armée*."

[123] The limit of self-defense to response to an armed attack is not universally accepted. *See* Tom J. Farer, *Political and Economic Coercion in Contemporary International Law*, 79 AM. J. INT'L L. 405 (1985).Professor Schachter has responded to such assertions forcefully and convincingly:

> Some commentators have gone so far as to contend that economic action of such intensity and magnitude would justify forcible self-defense by the target state, and collective defense by its allies. I disagree. Even egregious economic aggression whether or not illegal, does not constitute an armed attack or a use of force in

> the Charter sense. Allowing forcible reprisal to non-military coercion would broaden the grounds for use of force to an intolerable degree.

Oscar Schachter, *In Defense of International Rules on the Use of Force*, 53 U. CHI. L.REV. 113, 127 (1986). *See also* Report of the International Law Commission on the Work of its Thirty-Second Session (1980), U.N. Doc. A/35/10, *reprinted in* [1980] II (2) Y.B.I.L.C. 53, n.176.

It is often said that acts of unarmed aggression also exist (ideological, economic, political, etc.), but even though they are condemned, it cannot be inferred that a state which is a victim of such acts is permitted to resort to the use of armed force in self-defense. Hence, these possibly wrongful acts do not fall within the purview of the present topic, since recourse to armed force, as analysed in the context of self-defence, can be rendered lawful only in the case of armed attack.

[124] Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *reprinted in* 2 JOHN MOORE DIGEST OF INTERNATIONAL LAW 411-12 (1906). The Caroline incident involved a Canadian insurrection in 1837. After being defeated, the insurgents retreated into the United States where they recruited and planned further operations. The Caroline, a naval vessel, was being used by the rebels. British troops crossed the border and destroyed the vessel. Britain justified the action on the grounds that the United States was not enforcing its laws along the frontier and that the action was a legitimate exercise of self-defense. *Id*. at 409-11.

[125] *See* International Military Tribunal (Nuremberg), Judgement and Sentences, 41 AM. J. INT'L L. 172, 205 (1947). There is significant state practice regarding assertions of anticipatory self-defense. Professor Bowett has noted a number of the earlier examples:

> Pakistan justified the entry of her troops into Kashmir in 1948 on this basis before the Security Council, an argument opposed only by India. Israel's invasion of Sinai in October, 1956, and June, 1967, rested on the same argument. The OAS has used the same argument in relation to the blockade of Cuba during the 1962 missile crisis. Several states have expressed the same argument in the Sixth Committee in connection with the definition of aggression and the UN itself invoked the principle of anticipatory self-defense to justify action by ONUC in Katanga in December, 1961, and December, 1963. Following the invasion of Czechoslovakia by the USSR in 1968, it is permissible to assume that the USSR now shares this view, for there certainly existed no "armed attack."

Derek W. Bowett, *Reprisals Involving Resort to Armed Force*, 66 AM. J. INT'L L. 1, 4 n.8 (1972).

[126] *See, e.g.*, Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1634-35 (1984).

[127] Professor Dinstein perceptively notes that Article 2 of the Definition of Aggression Resolution refers to the first use of force as prima facie evidence of aggression. In other words, the burden is upon the actor to demonstrate that its use of force was not aggression. But this necessarily means that there are first uses of force that do not amount to aggression and are, therefore, not wrongful. *See* Dinstein, *supra* note 46, at 187.

[128] *Id.* at 190.

[129] "C3" refers to command, control, and communications systems. Similar terms of art include "C2," command and control, and "C3ISR," command, control, communications, intelligence, surveillance, and reconnaissance. "C2W," command and control warfare, would include attacks on systems encompassed by each of these terms. *See supra* note 11 and accompanying text

[130] Michael Walzer has suggested a similar line of reasoning:

[131] Self-defense must be both necessary and proportional. "There is a specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law." 1968 I.C.J. 4, 94 *cited with approval in* Legality of the Threat or Use of Nuclear Weapons, 1996 I.C.J. 4, 226, at para. 41, 31 I.L.M. 809, 822 (1996). *See also* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 905 (1987). Profess

[132] In 1980, the International Law Commission catalogued some of the more important and influential positions on the subject. Among those advocating limiting the right to situations involving armed attack were: J.L. Kinz, *Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations*, 41 AM. J. INT'L L. 872 (1947); Hans Kelsen, *Collective Security and Collective Self-Defense under the Charter of the United Nations* 42 AM. J. INT'L L. 783, 791-92 (1948); PHILIP JESSUP, A MODERN LAW OF NATIONS 165 (1948); Quincy Wright, *The United States Intervention in Lebanon*, 53 AM. J. INT'L L. 112 (1959). Taking the contrary approach were JAMES BRIERLY, THE LAW OF NATIONS 416 (1963); L.C. Green, *Armed Conflict, War and Self-Defence*, 6 ARCHIV DES VÖLKERRECHTS 387 (1957); MYRES MCDOUGAL & FREDERICO FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER 263 (1961). The ILC took no position on the issue.

[133] McDougal & Feliciano, *supra* note 132, at 207-08.