7-1-1998

Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?

Lloyd J. Matthews Colonel

CHALLENGING THE UNITED STATES SYMMETRICALLY AND ASYMMETRICALLY: CAN AMERICA BE DEFEATED?

Lloyd J. Matthews
Editor

July 1998

U. S. Army War College
Strategic Studies Institute
Carlisle Barracks, Pennsylvania

******

The views expressed in this book are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This book is cleared for public release; distribution is unlimited.

******

Comments pertaining to this book are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA 17013-5244. Comments also may be conveyed directly to the Conference Organizer, Dr. Earl H. Tilford, Jr., by calling commercial (717) 245-4086 or DSN 242-4086. Copies of this book may be obtained from the Publications and Production Office by calling commercial (717) 245-3820, or via the Internet at rummelr@awc.carlisle.army.mil

******

Selected 1993, 1994, and most later Strategic Studies Institute (SSI) publications are available on the Strategic Studies Homepage for electronic dissemination. SSI's Homepage address is: http://carlisle-www.army.mil/usassi/welcome.htm

TABLE OF CONTENTS

FOREWORD

The U.S. Army War College's Ninth Annual Strategy Conference was held at Carlisle Barracks, Pennsylvania, during the period March 31-April 2, 1998. The theme of the conference was "Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?" There were some 150 attendees, including active duty military personnel as well as members of academe, the U.S. Defense and service departments, think tanks, corporations, and news media.

This book is an outgrowth of that conference, though it makes no effort to present a comprehensive and literal record of events in the mold of traditional colloquium "proceedings." Rather, the book is organized as an anthology of selected conference presentations, complemented by sufficient notice of roundtable and question-and-answer discussion to provide a glimpse of the vigorous interplay of ideas evoked by this most timely of topics.

LARRY M. WORTZEL
Colonel, U.S. Army
Director, Strategic Studies Institute

PRELIMINARY OBSERVATIONS: ASYMMETRICAL WARFARE AND THE WESTERN MINDSET[1]

Charles J. Dunlap, Jr.

The concept of asymmetrical warfare is a popular and much discussed issue in U.S. defense literature these days. *Joint Vision 2010* (*JV 2010*),[2] the *Quadrennial Defense Review* (QDR),[3] and the *National Military Strategy* (NMS)[4] are just a few of the documents that express concern about it. Understandably, the Secretary of Defense has made addressing the phenomenon a central theme of his administration.

All of that said, what exactly is meant by asymmetrical warfare? In broad terms it simply means warfare that seeks to avoid an opponent's strengths; it is an approach that tries to focus whatever may be one side's comparative advantages against its enemy's relative weaknesses.[5] In a way, seeking asymmetries is fundamental to all warfighting. But in the modern context, asymmetrical warfare emphasizes what are popularly perceived as unconventional or nontraditional methodologies.

For most potential adversaries, attacking the United States asymmetrically is the only warfighting strategy they might reasonably consider for the foreseeable future. The Gulf War was an object lesson to military planners around the globe of the futility of attempting to confront the United States symmetrically, that is, with like forces and orthodox tactics.

In this essay I briefly examine how the West's cultural disposition and mindset affect its concept of asymmetrical warfare. I contend that the West's current focus may leave it vulnerable to asymmetrical challenges that arise from opponents whose cultural perspective differs significantly from that of the West.

Technology-Oriented Asymmetries.

In the West in general, and America in specific, asymmetrical warfare is frequently conceived in technological terms. *JV 2010* states, for example, that "our most vexing future adversary may be one who can *use technology* to make rapid improvements in its military capabilities that provide asymmetrical counters to US military strengths. . . ."[6] Unsurprisingly, therefore, weapons of mass destruction and information warfare are often proffered as illustrations of the asymmetrical warfare genre.[7]

The technological orientation of the Western mindset is to be expected. In his book, *On the Origins of War*, Donald Kagan writes that the scientific revolution ongoing since the 16th century has had a profound effect on the West. As a result, he maintains,

> It is a special characteristic of the modern Western world, as opposed to other civilizations and the premodern Western world, to believe that human beings can change and control the physical and social environment and even human nature.[8]

In due course, faith in the efficacy of technology and scientific methodology invaded thinking about warfare. That technology proved important to the military dominance of the West for over a century only reinforces the idea that it will continue to drive military success in the future.[9]

Furthermore, focusing on technology reflects the quintessential American approach to waging war. Historians Allan R. Millett and Peter Maslowski declare that since the mid-19th century (but particularly in the 20th century) the United States has relied upon "increasingly sophisticated technology to overcome logistical limitations . . . and to match enemy numbers with firepower."[10] This emphasis comports with America's sense of itself. The comments of General George S. Patton, Jr., typify the classic American view:

> The Americans, as a race, are the foremost mechanics of the world. . . . It therefore behooves us to devise methods of war which exploit our inherent superiority. We must fight the war by machines on the ground, and in the air, to the maximum of our ability.[11]

This concentration on technology continues today. *JV 2010*, the "operationally based template"[12] as to how America will fight future wars, centers on the question of how to "leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."[13] Clearly, the American "mindset" (if not that of the West generally) tends to see all difficulties—even the complex challenge of war—as technical problems subject to engineered solutions.[14]

Culturally-Oriented Asymmetries.

War does, of course, present technical problems but is not itself one. It is instead a contest of human wills that transcends the logic of the physical sciences. Importantly, it is also more than simply a violent form of a Westernized notion of politics. Indeed, the Clauswitzean mantra of the U.S. defense establishment, i.e., that war is an extension of politics by other means, has been much deconstructed by the work of John Keegan and others who address war's cultural basis.[15]

Complementing Keegan's thesis is that of Samuel Huntington. He argues that future conflicts will likely be clashes between civilizations with fundamentally different psychological orientations and value sets. Huntington maintains that certain ideas define what it is to be Western, and therefore add to what might be called the "Western mindset." These include such concepts as "individualism, liberalism, constitutionalism, human rights, equality, liberty, the rule of law, democracy, free markets, [and] the separation of church and state." [16]

What is important about Huntington's work is that he reminds us that the rest of the world does not necessarily

share these values. Thus, we should not expect that they will think the same way as the West about many subjects, including warfare. Lieutenant General Li Jijuan of the Chinese People's Liberation Army recently observed that "each civilization has its own notion of war which cannot help but be influenced by its cultural background."[17]

Nevertheless, an appreciation for the fact that other civilizations may look at war from a fundamentally different perspective is not only unknown to many in the West (and Americans especially) but wholly counter-intuitive to them. Americans persistently seem to assume that other peoples think basically the same as they do. Along these lines, Edward L. Rowney, a retired Army lieutenant general and former U.S. arms control negotiator, commented recently that:

> Our biggest mistakes stem from the assumption that others are like us, when in fact, they are more unlike than like us. We insist on ascribing to others our cultural traits, not recognizing that we have different objectives due to our unique historic backgrounds and sets of values. In short, "We fail to place ourselves in the other person's moccasins."[18]

When this obtuseness towards the mindset of our adversaries is allowed to affect strategic thinking, asymmetries result. H. R. McMaster argues in his book, *Dereliction of Duty*, for example, that the graduated application of airpower during the Vietnam War—intended to signal our resolve to support South Vietnam yet do so in a way that the United States believed demonstrated restraint—wholly misperceived North Vietnamese thought processes. McMaster contends:

> Graduated pressure was fundamentally flawed. . . . The strategy ignored the uncertainty of what was *the unpredictable psychology of an activity that involves killing, death, and destruction.* To the North Vietnamese, military action, involving as it did attacks on their forces and bombing their territory, was not simply a means of communication.

> Human sacrifice in war evokes strong emotions creating a dynamic that defies systems analysis quantification.[19]

The technological orientation of the Western mindset along with the assumed universality of Western values distorts the analysis of asymmetrical warfare. Consider the potential dangers of technology-based asymmetries. The West readily examines them because solving that kind of problem plays to the West's own notion of its comparative advantage, i.e., in the areas of weapons innovation and production. Such perceived "technological" asymmetries are almost welcomed by the West's military-industrial complex.

The much-ballyhooed Revolution in Military Affairs (RMA) exemplifies this trend. The RMA seeks to produce radically more effective militaries through the widespread application of emerging technologies, especially advanced computer and communications systems.[20] While it provides enormous opportunities for sales of new equipment to Western forces fearful of technological obsolescence, much of the new weaponry too often seems optimized for high-tech, peer-competitor war. In other words, it is aimed principally at a form of warfare that is symmetrical (in relation to the West) in its essence. In truth, few potential adversaries will wage symmetrical, high-tech war against the United States because doing so presents enormous training, logistical, and resource requirements, and these are "demands that few societies can meet."[21]

The characterization of weapons of mass destruction (WMD) as asymmetrical threats is a further manifestation of the West's analytical distortion. In truth, the premise that WMD constitute asymmetrical threats *vis-à-vis* the West—at least insofar as inter-state war is concerned—deserves challenge.[22] Given the West's still-sizable nuclear arsenals and its *relatively* robust capability to deal with other-than-nuclear WMD warfare, are WMD really asymmetrical to the West? So long as the West maintains its current capabilities, it seems rather unlikely that an

adversary could *decisively* employ WMD against it. In a very real sense, using WMD against the United States and other Western nations would represent an ill-considered attempt to match the West *symmetrically*.

The use of WMD in the context of terrorism committed by non-state actors is, of course, a profound and different challenge. As serious a problem as terrorism is—especially when WMD are involved—it is not likely to actually defeat the West. It does not yet appear that non-state actors could mount a sufficiently comprehensive attack to physically vanquish a nation like the United States. Martin Van Creveld has pointed out that terrorism has never succeeded in the West because the nature of modernity is that it provides redundancies that give advanced societies resiliency against the sort of sporadic attacks that terrorists carry out, even though individual incidents might be quite costly.[23]

The "Real" Asymmetrical Challenge .

Quite clearly, terrorism principally aims to affect its targets more *psychologically* than physically. To that extent it does suggest the real asymmetrical challenge for the West. Major General Robert H. Scales, Jr., the Commandant of the Army War College, argues that in future conflicts an enemy may perceive his comparative advantage against the United States and the West not in technological terms, but in the "collective psyche and will of his people."[24] In turn, this generates an obvious question, i.e., how will an enemy attack the West's psyche and will? The answer makes Americans and others in the West uncomfortable because it raises the specter that basic Western values, the very things Huntington sees as defining the West, are in fact the asymmetries that future adversaries will most likely seek to exploit.

The potential asymmetrical vulnerabilities about which the West should be concerned are not so much technological as the Western mindset believes (and even prefers), but

rather are those that turn the fundamentals of the West's culture and political system against itself. For example, among the things that adversaries have learned in the latter half of the 20th century is to exploit the West's democratic system. Consider the remarks of a former North Vietnamese commander: "The conscience of America was part of its war-making capability, and we were turning that power in our favor. America lost because of its democracy; through dissent and protest it lost the ability to mobilize a will to win."[25] Thus, by stirring up dissension in the United States, the North Vietnamese were able to advance their strategic goal of removing American power from Southeast Asia.

More recently, by dragging the body of a U.S. soldier through the streets of Mogadishu, the Somalis were able to destroy the public support upon which the United States and other Western democracies depend upon to sustain military operations. We should expect such strategies to proliferate as new communications technologies vastly enhance the newsgathering and dissemination capabilities of international media organizations.[26]

Enemies may perceive vulnerable asymmetries in what the West views as its virtues. While the mindset in the United States and the West sees, as *JV 2010* says, the "moral strengths" and the "ethical standards" of its troops as keys to military power,[27] adversaries willing to abandon Westernized legal and ethical regimes may well consider them as things to exploit and manipulate.[28] Increasingly, opponents will seek to present Western militaries with moral and ethical conundrums. For example, the Serbs were able to discourage high-tech NATO air attacks by the simple expedient of chaining hostage UN troops to potential targets.[29] The idea of purposely killing friendly troops in order to destroy an enemy target will be very difficult for Western forces to rationalize.

Where once the "Western way of war" meant that adversaries risked wars often characterized by decisive

battles where the annihilation of enemy forces was sought,[30] today we see the emergence of a Western mindset markedly more sensitive to casualties on *both* sides.[31] Enemies may consider this humanitarian concern as yet another asymmetry on which they can capitalize in ways the Western mindset considers unthinkable: they may purposely put their own people in jeopardy if doing do complicates or adversely affects the West's use of its military power.

Indeed, Somali warlords used women and children as human shields against coalition forces during the intervention of the early 1990s. Along similar lines, the Libyans have threatened to encircle a facility alleged to be involved with the production of weapons of mass destruction with "millions of Muslims" in order to deter attacks by the West.[32] Most recently, when Western military action seemed imminent, Saddam Hussein surrounded his palaces and other buildings with noncombatant civilians (some of whom may have genuinely volunteered) in order to discourage attacks by Western forces sensitive to the effect on their publics of civilian deaths, regardless of the circumstances.[33] Analyst James F. Dunnigan cautions that "if the opponents are bloody-minded enough, they will always exploit the humanitarian attitudes of their adversaries."[34]

Even those opponents—including possible peer competitors—who seek to achieve technological asymmetries over the West may likewise find it profitable to use our values against us. The West's free-market, open-competition economic system encourages innovation and quickly produces technological advances. But the nature of that system in a democracy makes turning new ideas into deployed weapons a cumbersome and lengthy process—something extremely worrisome in an age of rapid technological change.

An adversary less constrained by the political realities of a capitalistic democracy may be able to gain an

asymmetrical advantage by deploying the latest systems more rapidly than can the bureaucratically-restrained Western militaries. Author David Shukman explains:

> While the Western military struggles for a decade on average to acquire new weapons, a country with commercially available computer equipment and *less rigorous democratic and accounting* processes could field new systems within a few years. It is the stuff of military nightmares.[35]

Parenthetically, it is unlikely that the openness of democratic societies will allow the achievement of an asymmetrical advantage via technological surprise against future adversaries, despite the West's best efforts. Ephraim Kam asserts in *Surprise Attack* that "since it takes a long time to produce and deploy new weapons in sufficient quantities capable of changing the military balance between nations, information on their characteristics usually becomes available in the interim."[36] While many opponents will lack the resources to develop technologically superior countermeasures, they may nevertheless be able to develop low-tech offsets as has been done with some regularity in the past.

In fact, an over-emphasis on technology can cause the West to overlook the many low-tech ways in which adversaries might asymmetrically respond to gadgetry-obsessed—and gadgetry-vulnerable—Western opponents.[37] What is so remarkable about this is that so few seem to remember the lessons of relatively recent history. Two senior U.S. military commanders warn against the siren song of technology in the Autumn 1997 issue of *Parameters*. They point out that:

> [Technological] supremacy could not prevent Holland's defeat in Indonesia, France's defeats in Indonesia and Algeria, America's defeat in Vietnam, the Soviet Union's defeat in Afghanistan, or Russia's more recent defeat in Chechyna. All these episodes confirm that technological superiority does not automatically guarantee victory on the battlefield, still less the negotiating table.[38]

Future adversaries may wage asymmetrical warfare by combining available low-tech equipment with a culturally-oriented strategy. For example, Marines should expect to face opponents who deploy relatively unsophisticated mines, much as Iraq did during the Gulf War, in the hopes of replicating the Iraq's success in deterring an amphibious assault following damage by mines to the U.S.S. *Tripoli* and the U.S.S. *Princeton*.[39] Similarly, opponents will likely acquire small, diesel-powered submarines to present the same threat.[40] What is important here is that such schemes might not be able to stop a determined assault, but an adversary may intend to simply exploit the growing aversion to casualties in the West's culture by causing some losses which would, in turn, erode support for the West's military effort.

Surface ships may face an even more insidious threat: an enemy could use a civilian airliner covertly loaded with explosives to launch an attack on a high-value target such as an aircraft carrier. The plane might be flown by a suicide pilot (or automatically guided) and carry a hostage or even volunteer group of civilian passengers. Recalling the recriminations that followed the accidental shootdown of an Iranian airliner by the cruiser *Vincennes*,[41] the adversary may hope to create just enough hesitation on the part of the ship's crew to allow the aircraft to successfully penetrate the defenses. Again, simply causing casualties—in this scenario both U.S. military personnel and enemy civilians—would be the aim.

It is paradoxical that these kinds of enemy actions against forward deployed American forces might engender a completely different reaction than acts of terrorism against the U. S. homeland. Although the objective of both might be to maximize casualties, the former could succeed in undermining public support for an overseas operation while the latter may well evoke a demand for extreme measures against the perpetrators. Such is the mercurial nature of contemporary U.S. public opinion.

In any event, the kind of asymmetrical warfare future adversaries may wage is not that which seeks to actually defeat U.S. or Western military forces, but rather that which assaults the psyche and will of the populations whose political support is required by Western democracies to sustain military operations.

Conclusions.

Hopefully, this essay will not be interpreted as an anti-technology, Luddite manifesto. To the contrary, no one—least of whom the author—disputes the dictum that "technology and warfare have never been far apart."[42] Moreover, it is unquestionably true that decisionmakers must be extremely concerned about procuring the finest technology for U.S. forces. Analysts Ronald Haycock and Keith Neilson warn that to a great extent military applications of technology have "permitted the division of mankind into ruler and ruled."[43] And it is also still true that technology is the West's comparative advantage.

One of the great dangers, however, is that decisionmakers may delude themselves into thinking that the challenge of asymmetrical warfare is *exclusively* technological. It is especially a concern as more and more of the civilian leadership lack first-hand military experience. This has led some military officers to worry, as the *Wall Street Journal* reported in 1995, that such leaders might believe that "gadgets can somehow substitute for the blood and sweat of ground combat."[44]

The West must recognize that consideration of war as a technological or engineering problem has its limits. The engineer's culture is an "aggressively rational one" where technical problems are solved with a logical application of scientific principles."[45] War, however, is something different. Lieutenant General Paul K. Van Riper, USMC, explains:

> Technology permeates every aspect of war, but the science of war cannot account for the dynamic interaction of the physical and moral elements that come into play, by design or by chance, in combat. War will remain predominately an art, infused with human will, creativity, and judgment.[46]

What is necessary for the United States and the West is to expand its assessment of asymmetrical warfare. Asymmetrical warfare needs to be examined from the culturally distinct perspective of potential enemies. As unpleasant as it may be, the West must consider that enemies may try to turn against us the very values that the West is seeking to protect. In particular, the United States and the West must not allow its technologically-oriented mindset to blind it to the fact that modern war remains, as already noted, a struggle of psyches and wills.

The West must be prepared to meet the moral as well as technical challenge of future war. Enemies may concede that physically defeating the military the forces of the United States and the West is beyond their capability, but nevertheless attempt to achieve their war aims by overcoming the West's will, testing it in new and innovative ways. That is the essence of the challenge of asymmetrical warfare in the 21st century. To the extent that we indulge ourselves with visions that success in future war can be reduced to finding high-tech "silver bullets," all that the West holds dear is in peril.

ENDNOTES

1. Presented originally on November 20, 1997, in Cambridge, MA, to "The Role of Naval Forces in 21st Century Operations" Conference sponsored by the Fletcher School of Law and Diplomacy of Tufts University, the Institute for Foreign Policy Analysis, the Commandant of the U.S. Marine Corps, and the Chief of Naval Operations, U.S. Navy.

2. Chairman of the Joint Chiefs of Staff, *Joint Vision 2010,* 1996.

3. William S. Cohen, *Report of the Quadrennial Defense Review*, May 1997.

4. Chairman of the Joint Chiefs of Staff, *National Military Strategy of the United States of America,* September 1997.

5. Other authorities define asymmetrical warfare somewhat differently. For example, in its unclassified report on the exercise STRATEGIC FORCE '96, the Air Force discussed the issue as follows:

> The symmetrical battles have classically pitted steel against steel in slow wars of attrition. Asymmetrical warfare departs from this thinking. Asymmetrical warfare avoids traditional force-on-force battles. Asymmetrical warfare favors pitting your strength against an enemy's strength or weakness in a nontraditional and sometimes unconventional manner.

Department of the Air Force, *Strategic Force*, 1997, p. 8.

6. See *JV 2010,* pp. 10-11.

7. See, e.g., *ibid.,* p. 11, (information technologies); *QDR,* p. 4, (NBC [nuclear, biological, and chemical] threats, information warfare); and *NMS,* p. 9, (WMD and information warfare).

8. Donald Kagan, *On the Origins of War and the Preservation of Peace*, 1995, p. 3.

9. See Michael Howard, *War in European History*, 1976, pp. 116-135.

10. Allan R. Millett and Peter Maslowski, *For the Common Defense*, 2d ed., 1994, p. xii.

11. As quoted by Colin S. Gray, "U.S. Strategic Culture: Implications for Defense Technology" in Asa A. Clark IV and John F. Lilley, eds., *Defense Technology*, 1989, p. 31.

12. *JV 2010,* p. ii.

13. *Ibid.,* p. 1.

14. See Robert N. Ellithorpe, *Warfare in Transition? American Military Culture Prepares for the Information Age*, a presentation for the Biennial International Conference of the Inter-University Seminar on Armed Forces and Society, Baltimore, MD, October 24-26, 1997, p. 18 (unpublished paper on file with author). ("American military culture historically emphasized scientific approaches to warfare to the point of

holding an almost mystical belief in the power of technology to solve the challenges of war.")

15. See John Keegan, *A History of Warfare*, 1993. Harry Summers maintains that Keegan makes a false distinction between "politics" and "culture." See Colonel Harry G. Summers, Jr., USA, Ret., *The New World Order*, 1995, pp. 40-42.

16. See Council on Foreign Relations, *The Clash of Civilizations? The Debate*, 1996. Huntington has expanded his thesis to a book-length treatise entitled *The Clash of Civilizations and the Remaking of World Order*, 1996.

17. Lieutenant General Li Jijuan, *Traditional Military Thinking and the Defensive Strategy of China*, LeTort Paper No. 1, U.S. Army War College, Strategic Studies Institute, Earl Tilford, ed., August 29, 1997, p. 1.

18. Edward L. Rowney, "Tough Times, Tougher Talk," *American Legion Magazine*, May 1997, pp. 24-26.

19. H. R. McMaster, *Dereliction of Duty*, 1997, p. 327, emphasis added.

20. For discussions of "the revolution in military affairs" in the information age, see generally "Select Enemy. Delete.," *The Economist*, March 8, 1997, p. 21; Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs*, March/April 1996, p. 37; Andrew F. Krepinevich, "Cavalry to Computers: The Pattern of Military Revolutions, *The National Interest*," Fall 1994, p. 30; and James R. Fitzsimonds and Jan M. Van Tol, "Revolutions in Military Affairs," *Joint Force Quarterly*, Spring 1994, p. 24.

21. Geoffrey Parker, "The Future of Western Warfare," in Geoffrey Parker, ed., *Cambridge Illustrated History of Warfare*, 1995, p. 369.

22. Military historian Martin Van Creveld makes the interesting observation that, ironically, "in *every* region where [nuclear weapons] have been introduced, large-scale, interstate war has as good as disappeared." Martin Van Creveld, "Technology and War II," in Charles Townsend, ed., *The Oxford Illustrated History of Modern War,* 1997, p. 304, emphasis in original.

23. Martin Van Creveld, *Technology and War*, Rev. Ed., 1991, pp. 307-308.

24. As quoted by James Kittfield, in "The Air Force Wants to Spread Its Wings," *National Journal*, November 8, 1997, p. 2264.

25. As quoted in "How North Vietnam Won the War," *The Wall Street Journal*, August 3, 1995, p. A8.

26. Douglas Waller, a *Time Magazine* correspondent, observes:

> The same technology that is revolutionizing the way the Pentagon fights wars is also changing the way the media cover them. The media can now provide viewers, listeners and even readers almost instant access to a battlefield. With lighter video cameras, smaller portable computers, cellular phones, their own aircraft, and worldwide electronic linkups, the media can report on any battlefield no matter how remote and no matter how many restrictions the Defense Department tries to place on coverage.

Douglas Waller, *Public Affairs, the Media, and War in the Information Age,* a presentation for the "War in the Information Age" Conference, Tufts University, November 15-16, 1995 (unpublished paper on file with author).

27. *JV 2010*, pp. 28, 34.

28. In a fascinating piece in *Parameters*, Ralph Peters, then a U.S. Army major, described what he called the rise of "The New Warrior Class," a multitude which he contends "already numbers in the millions." Peters says that in the future,

> [America] will face [warriors] who have acquired a taste for killing, who do not behave rationally according to our definition of rationality, who are capable of atrocities that challenge the descriptive powers of language, and who will sacrifice their own kind in order to survive.

Ralph Peters, "The New Warrior Class," *Parameters*, Summer 1994, p. 24.

29. See Lieutenant Colonel Thomas X. Hammes, "Don't Look Back, They're Not Behind You," *The Marine Corps Gazette*, May 1996, pp. 72-73, discussing the military implications of chaining hostages to targets. Hostage taking was not clearly prohibited until after World War II. See H. Wayne Elliot, "Hostages or Prisoners of War: War Crimes at Dinner," *Military Law Review*, Vol. 149, Summer 1995, pp. 241-274.

Hostage taking appears to be an effective tactic. See, *e.g.,* Stephen Erlanger, "Russia Allows Rebels to Leave with Hostages," *New York Times*, June 20, 1995, p. 1. ("Nearly all the demands of Chechens are met.")

30. See, generally, Victor Davis Hanson, *The Western Way of War*, 1989; Doyne Dawson, *The Origins of Western Warfare*, 1996; and Russell E. Weigley, *The American Way of War*, 1973.

31. Walter J. Boyne notes "two unique demands that have since Vietnam come to be made by the American public":

> The first of these demands is that we must fight our wars with a minimum of casualties to our forces. America wants no more Vietnams where our troops are forced to fight and die in unconscionable numbers. The second of these demands is unusual in history, for it is that we must also win our wars with a minimum number of casualties inflicted on the enemy.

Walter J. Boyne, *Beyond the Wild Blue: A History of the U.S. Air Force 1947-1997*, 1997, p. 7.

32. See "Libyans to Form Shield at Suspected Arms Plant," *Baltimore Sun*, May 17, 1996, p. 14.

33. See Barbara Slavin, "Iraq Leaves U.S. Few Options," *USA Today*, November 14, 1997, p. 13A.

34. James F. Dunnigan, *Digital Soldiers: The Evolution of High-Tech Weaponry and Tomorrow's Brave New Battlefield*, 1996, p. 219.

35. See David Shukman, *Tomorrow's War: The Threat of High-Technology Weapons*, 1996, p. 8. See also Michael Loescher, "New Approaches to DoD Information-Systems Acquisition" in *Cyberwar: Security, Strategy and Conflict in the Information Age*, Alan D. Campen, *et al*., eds., 1996, p. 127 ("In a world in which state-of-the-art is off-the-shelf, industry, and potentially our foes, can obtain better information systems, technology cheaper and faster than DoD because our current acquisition system buys computers in the same way we buy bullets"); and Jeffery R. Barnett, *Future War*, 1996, p. 17, stressing the need to compress the procurement time for information technologies.

36. Ephraim Kam, *Surprise Attacks*, 1988, p. 19.

37. See, *e.g.,* Charles J. Dunlap, Jr., "How We Lost the High-Tech War of 2007," *The Weekly Standard*, January 29, 1996, p. 22.

38. Lieutenant General Paul K. Van Riper, USMC, and Major General Robert H. Scales, Jr., USA, "Preparing for War in the 21st Century," *Parameters*, Autumn 1997, pp. 4-5.

39. Although the absence of an amphibious assault during the Gulf War was later characterized as a deception operation, General Schwarzkopf's memoirs make it clear that concerns about mines were key. See General H. Norman Schwarzkopf, *It Doesn't Take a Hero*, 1992, p. 446. See also Rick Atkinson, *Crusade*, 1993, pp. 239-240.

40. For a discussion of how a few submarines can complicate a military operation, see, generally, Admiral Sandy Woodward, *One Hundred Days*, 1992 (Falklands War).

41. On July 3, 1987, the cruiser U.S.S. *Vincennes* shot down Iranian Air flight 655 over the Persian Gulf when it mistook the civilian aircraft for a military threat. Killed were 224 adults and 65 children. See Sandra Mackey, *The Iranians*, 1996, p. 331.

42. Ronald Haycock and Keith Neilson, *Men, Machines, and War*, 1988, p. xi.

43. *Ibid.*, p. xii.

44. Thomas E. Ricks, "Gingrich's Futuristic Visions for Re-Shaping the Armed Forces Worry Military Professionals," *Wall Street Journal*, February 8, 1995, p. 16.

45. Robert Poole, *Beyond Engineering*, 1997, p. 209.

46. Lieutenant General Paul K. Van Riper, "Information Superiority," *Marine Corps Gazette*, June 1997, pp. 54, 62.

PART I:
SYMMETRIES AND ASYMMETRIES—
A HISTORICAL PERSPECTIVE

INTRODUCTION

Lloyd J. Matthews

Asymmetry—is it not a hot new buzzword equivalent for such prosaic terms as difference, disparity, disproportion, imbalance, etc.? Not really. Understanding asymmetry in today's military parlance begins with the unremarkable fact that every state—from the most modern to the most primitive—has both advantages and disadvantages in waging war with another state, regardless of the relative levels of advancement of the two.

To cite an extreme and purely hypothetical illustration, suppose a powerful modern force from an advanced Western industrial nation undertakes to subdue a small tribal state of spear-throwing goatherds living at elevations above 15,000 feet in mountain clefts and caves. In brute military terms, the moderns at first glance appear to have every conceivable advantage. On further study, however, analysts note that the goatherds do have a few modest factors in their favor: they are physically acclimated to working in the cold, oxygen-depleted environment; their food supply is simple, at hand, and well-nigh inexhaustible; their hideouts and caches are impossible to locate from the air; and the roadless, torturously steep terrain is inhospitable to any vehicle but the foot.

After returning to their books, maps, and charts a second time, the analysts arrive at the disconcerting realization that the "modest" advantages enjoyed by the goatherds are in fact quite likely to prove decisive, and that it will be inordinately difficult for the contemporary force to subdue the primitives at a price anyone regards as politically

acceptable. In the wondrous calculus of asymmetrics, then, we find that the advantages accruing to the modern force are neutralized and the disadvantages enormously magnified, while the precise converse becomes true for the backward force in essence only a few decades removed from the Paleolithic age.

In formal terms, we can define asymmetry as any militarily significant disparity between contending parties with respect to the elements of military power broadly construed. Asymmetrics invites study of the fact that elements of military power are never applied in a vacuum, but always in particular political, economic, cultural, religious, psychological, geographic, and climatic contexts that qualify the utility of each element of power and condition the way each acts against the other elements of power. The process of calculating the resultant of the various vectors of power wielded by two asymmetrically related opponents—in order to measure the dimensions of the threat that each poses to the other—can be quite problematic. But it is a process that must be undertaken if we are to give due weight to all the relevant elements of power.

Because of its deeper level of analysis, the insights revealed by asymmetrics are not always congruent with common sense and received wisdom, which usually derive from surface appearances. For example, there has been a consistent leaning by Western observers toward the complacent conviction that great national wealth; large, technologically advanced forces; and a proud martial tradition will automatically translate to victory over the untutored, unwashed warriors of the lesser world. However, since contemporary forces are trained and equipped to fight forces much like themselves, when they encounter instead a markedly asymmetric foe—one judged to be objectively inferior—they have frequently shown an inability or unwillingness to make the adaptations, adjustments, and compromises needed to cope with the unfamiliar modes of resistance. The French experience in Vietnam, 1946-54, the

United States in Vietnam, 1959-73, the Soviet Union in Afghanistan, 1979-89, and the United States again in Somalia, 1992-94, all reveal to some degree how the commonsense view of relative military power can lead us astray.

Since American armed forces are unlikely to encounter a mirror image (i.e. symmetrical) opponent on the battlefield in the near to mid term, prudent strategy demands that we devote substantial attention to the remaining potential military threat to national security—that posed by an asymmetric opponent. We begin this process with Part I—Symmetries and Asymmetries: A Historical Perspective. Here, we find three studies that explore in detail how selected armed forces of the past have grappled with the perplexities of fighting an opponent cast from a markedly different mold.

From the large catalogue of factors contributing to military power, Dr. John F. Guilmartin, Jr., in "Technology and Asymmetrics in Modern Warfare" focuses upon the factor that commands the lion's share of attention in virtually all discussions of the Revolution in Military Affairs—technology. Dr. Guilmartin first takes care to distinguish between high tech (a qualitative distinction based on technological sophistication and capability) and high end (a quantitative distinction based on size, cost, and complexity). He illustrates these distinctions, along with discussion of their implications for success in war, with a historical *tour d'horizon* going back to the early 16th century and even beyond.

The thematic center of the paper is an incisive treatment of the role of asymmetrical technology in the Spanish overthrow of the Aztec and Inca empires, 1519-1539 (as amplified in an appendix). Arguing that the experiences of Cortés and Pizarro still have relevance today, Dr. Guilmartin concludes that "the dramatic asymmetry in weaponry, though a necessary condition for Spanish victory, was not a sufficient one, and that an understanding

of the interplay among political, psycho-social, and technological considerations is needed to explain the conquistadors' success."

In an interesting departure from the usual approach to asymmetric studies, Colonel Robert A. Doughty in "The Myth of the *Blitzkrieg*" revises the long-accepted notion that the decisive German victory over France in 1940 was the result of a revolutionary new doctrine of war denominated as "Blitzkrieg"—one that putatively gave the Germans an asymmetrical edge over the French. Colonel Doughty demonstrates that prior to the campaign there was no coherent German concept of war envisioning lightning-like deep armor thrusts supported by air that would lead to quick victory. Instead, the victory was based upon "more traditional aspects of tactics, operations, strategy, and leadership," often relying on infantry rather than tanks or aircraft and marked by closely contested local encounters rather than fluid penetrations to distant operational objectives. In gross terms at least, the forces of these two modern industrialized nations were very much alike, and if any asymmetry did exist in favor of the Germans, it lay within the customary elements of military power. In Colonel Doughty's telling, the idea of "Blitzkrieg" as a revolutionary doctrinal triumph was manufactured after the fact as a tool of Nazi propagandists and as a device for adding luster to the reputations of German generals.

In "Asymmetric Response to American Air Supremacy in Vietnam," Professor Donald R. Mrozek focuses the lens of asymmetric study on the effectiveness of America's vaunted air power in its confrontation with the guerrilla and conventional forces of a third world foe in Vietnam.

As preclude to taking up the Vietnam question, Professor Mrozek surveys America's own considerable experience with asymmetric warfare, finding that despite the cautionary lessons readily available, America nonetheless cast its lot wholly with the Enlightenment tradition. Here was emphasized the superiority of a

rational, universalist, professional approach to waging war, as opposed to the impassioned improvisation of the insurgent mentality where concepts of pain, time, and victory were at stark variance with those of the West.

During the North Vietnamese siege of Khe Sanh in 1968, for example, U.S. aerial bombardment turned the circumference of the base into a celebrated killing ground where loss figures favored the allies by 8 to 1; yet, as Professor Mrozek points out, this was a mere eddy in a war that continued its remorseless flow toward North Vietnamese victory. Much the same could be said for site defense, interdiction, and sending political messages, in all of which roles massive U.S. air power was applied to ambiguous or overstated effect. At best, the United States used "its asymmetrical air power edge in ways that delayed but did not change the final outcome."

It was beyond the bounds of Professor Mrozek's topic for him to speculate on the larger question of how the war would have developed had U.S. political leaders opted from the beginning to exploit fully their massive asymmetric conventional edge by eschewing crippling controls on the pace and scope of air-ground-naval operations throughout the theater, while launching attacks directly against the North Vietnamese regime and sealing the borders of the South.

TECHNOLOGY AND ASYMMETRICS IN MODERN WARFARE

John F. Guilmartin, Jr.

Though the term is of relatively recent coinage, technological asymmetry in warfare has long held a fascination for military professionals, defense analysts, and military historians. That fascination has recently been sharpened by the ongoing debate over the posited existence, nature, and consequences of the so-called Revolution in Military Affairs, or RMA, that is generally (though by no means universally) held to have manifested itself during the 1990-1991 Gulf War. Though I have some strong views on the subject, I see little benefit in reviewing the RMA debate, not least of all because many, if not most of you in the audience are at least as familiar with the nuances of that debate as I. Suffice it to say that there is general agreement that advances in precision-guided weaponry, target acquisition and tracking devices, avionics, fire control systems, and secure communications, acting in combination with the development of stealth technology, have combined to raise warfare to new levels of lethality. The advantages of these technologies, of course, accrue only to those nations that have mastered them and posses the fiscal wherewithal to produce them in meaningful numbers. In practical terms, that means the United States, though certain of our allies share in the benefits.

My purpose in this paper is to identify the key technologies in question, briefly delineate their salient operational characteristics, develop a historically-based analytical framework within which to address and test the concept of an RMA, and then use that framework as a vehicle to identify and analyze selected case studies involving technological asymmetry with an eye to the future. My topic is not asymmetry in warfare—an enormous subject which will more than occupy us for the next two

days—but technological asymmetrics. Let me begin by offering my working definition of technology:

> **technology:** (1) the application of knowledge to achieve a physical effect by means of an artifact, object, or thing; (2) the artifact itself; the class of artifacts to which it belongs; or (3) the knowledge needed to design, manufacture, operate, sustain and logistically support the artifact or thing and its user(s).

Note that organizational schemes are technologies under my definition, the infantry division, for instance, or the cellular organization of a terrorist group. Note too that the physical effect might be indirect, as with intelligence analysis or weather forecasting.

Next, I have found it useful to distinguish between high tech and high end.[1] While the two concepts overlap, high tech is a qualitative distinction defined by technological sophistication and capability, while high end is defined by size, cost, and complexity. We can apply these distinctions at the level of individual systems or to entire organizations and facilities. An example of a high tech, low end system is a set of state-of-the-art night vision goggles or a Global Positioning System (GPS) indicator, though the GPS system as a whole is high tech, high end. An AK-47 or a hand grenade are examples of low tech, low end systems, while a third world infantry division would be low tech, high end and so on. Obviously, these distinctions change with time: an *Iowa* class battleship would have been high tech, high end in 1945 while the same vessel in the 1980s would have been low tech, high end or perhaps mid tech, high end taking into account the updated fire control system and missile armament.

With these definitions in mind, let me briefly review the salient Gulf War high tech systems commonly associated with the RMA to establish a frame of reference and make some preliminary observations on technological asymmetries. Heading the list in terms of operational impact is the wedding of sophisticated night vision devices to precision guided munitions and fire control systems.[2] In

the air, that translated most prominently into laser-guided bombs; on the ground the salient manifestation was the ability of the M1A1 main battle tank to achieve first round kills firing at night and on the move, though the night-capable AH-64 attack helicopter with its laser-guided Hellfire missiles deserves mention as well. Next comes the proliferation of secure communications that permitted the enormous amount of vertical communication and—particularly in the air war—lateral coordination needed to link strategy to operations and to make battle plans work. In practical terms, that meant secure telephones and facsimile machines, though one might add color Xerox machines under the general rubric of communications.[3] Then—and I do not pretend that my rank-ordering is definitive—come miniaturized navigation and guidance systems. At sea and in the air, these systems made the long-range, autonomous, precision-guided Navy Tomahawk Land Attack Missile TLAM) and Air Force Conventional Air Launched Cruise Missile (CALCM) a reality; on the ground, GPS indicators allowed U.S. to fire and maneuver with unprecedented precision and confidence.[4]

Next come low observables, aerial attack systems capable of passively defeating air defense radars, notably the F-117A stealth fighter, TLAM, and CALCM. One can make a good argument for bumping low observables up in the rank ordering, but I would note that stealthiness is a means to an end, not an end in itself. I would further note that the F-117's cutting edge is the infrared target acquisition and designator system for its laser-guided bombs and that much of the F-117's operational value in the Gulf War stemmed from its superior accuracy, in part a product of the fact that stealth pilots could afford the luxury of extended straight and level bomb runs.[5] In short, low observability is an enabling factor that multiplies the effect of other technologies. The notion of technological advantage as a tactical enabling factor is a theme to which I will return.

Next I would list a variety of technologies and munitions designed for the suppression of enemy air defenses (SEAD) mission; my primary reference is to the HARM (high speed anti-radiation missile) and the F-4G "Wild Weasel" fighter that kills SAMs (surface-to-air missiles), though we should add EF-111 and EA-6B jammers and decoy drones to the list. Advanced technologies that played comparatively lesser roles, but showed promise for the future include the Joint Surveillance Target Attack Radar System (JSTARS) and the night, adverse-weather, and adverse terrain-capable MH-53J Pave Low III helicopter.

To reiterate my initial point, the argument for the existence of an RMA stems in large measure from the effectiveness in the Gulf War of the kinds of systems noted above. That argument is strengthened by our continuing development of new systems in all of these categories and by experiments with more effective means of exploiting them, particularly those involving the digitized battlefield and its naval equivalents. I offer two notes of caution at this point. First, much of our tactical success in the Gulf War was attributable not just to superior technology, but to superior training as well, and in many cases it is difficult to say where one left off and the other began. The TLAM's success might appear to be purely technologically determined, but target selection and route planning, both dependent on user skill, were important determinants of effectiveness. The same point applies with even greater force to such systems as the F-117 and M1A1. Indeed, one might argue, with seeming perversity, that increased technological sophistication and capability are more likely to increase demands on user skill and training than to relax them. The importance of user skill and training is another theme to which I will return.

My second cautionary note is a reminder that much of our effectiveness in the Gulf War depended on low and medium tech, high end systems. Aerial refueling came of age as a powerful force multiplier, producing enormous operational and tactical flexibility far above and beyond

simple range extension.[6] Again, the value of refueling was multiplied by aircrew training, and here the advantage was not just, or even particularly, one of individual skill, but rather it was a collective phenomenon: the ability of U.S. tanker and tactical aircrews to quickly improvise refuelings in response to the unanticipated—adverse weather and tactical problems or opportunities—gave U.S. unmatched flexibility[7] and that flexibility was a product of sustained and realistic inter-unit training.

B-52s dropping large numbers of dumb bombs once again demonstrated their effectiveness against troop concentrations and industrial complexes. Venerable M-60 tanks in Marine hands proved remarkably effective. Aircraft carriers were awfully handy to have around, particularly in the early, nervous, days of DESERT SHIELD. We could not have done it without sealift. I could go on, but before moving on to the flip side of the RMA—and I use the term only as an accepted label—it is worth remembering that DESERT STORM would have been impossible without President George Bush's diplomacy. The importance of the diplomatic/military interface is another point to which I will return.

And now for the flip side. Hard on the heels of the wave of enthusiasm for our mastery of high tech warfare came a sober appreciation that such methods did not necessarily lend themselves to conflicts against low tech opponents lacking the traditional objectives, lucrative targets, and direct operational methods vulnerable to high tech weaponry. Indeed, even the Gulf War raised warning flags, among them our embarrassing difficulty in dealing with the threat caused by an antiquated Soviet mobile surface-to-surface missile system, the Scud.[8] The warning flags were raised to masthead level in the wake of the Mogadishu debacle, in which we lost 18 servicemen to a decidedly low tech enemy. Those with their hands on the halyards, unlike all too many high tech enthusiasts, clearly saw the political dangers arising from an over reliance on technological advantage acting in combination with our

peculiar social and political sensitivities as a nation. The ultimate expression of their concerns to date is the famous—dare I say notorious—article "How We Lost the High Tech War of 2007."[9] Its author, Air Force Colonel Charles Dunlap, explores idea that a ruthless low tech enemy might exploit our societal squeamishness for bloodshed and suffering to turn our tactical dependence on overwhelming high tech superiority into a lethal strategic liability.

With the above points in mind, I turn to the question of how technological asymmetrics actually play out in war. Clausewitz believed that a historical example was worth any amount of speculation,[10] and historical antecedents should at least provide us with meaningful questions to ask and hypotheses to apply. In preparing this paper, I was struck by the realization that the closest historical analog to the current RMA can be found in the remarkable advances in the Spanish practice of arms in the early 16th century. Forced to intervene in Italy in 1495 to thwart the ambitions of an expansive France, Spanish arms suffered initial defeat at the hands of Swiss pikemen and French heavy cavalry at the Seminara River. Under the inspired leadership of Gonsalvo de Cordova, the Spanish reworked their weaponry and tactics, adopting the pike and abandoning the crossbow in favor of increasingly powerful firearms. In remarkably short order, they had taken the measure of the superior shock power of Swiss pikemen and French gendarmes, defeating a French army at Cerignola in 1503.[11] To be sure, that victory owed much to Gonsalvo's clever use of terrain and field fortifications, a point seized on by professional critics.[12] It also owed much to the brutal effectiveness of Spanish light horse in pursuit, for *ginetes* (Spanish light cavalry armed with traditional weapons) had been sound from the beginning if not misused for shock action against heavier opponents.

The Spanish continued to refine their tactics and adjust their weaponry mix, and learned to fight in disciplined formations that combined shock action in the form of

pikemen with firepower in the form of arquebusiers and musketeers. These formations, initially called *columnas*, were the first dismounted units, certainly in modern times and to the best of my knowledge ever, capable of defeating superior numbers of competent and aggressive cavalry in open terrain—a point perceptive military professionals noted with awe.[13] This was a revolutionary change, horse archers having been slicing up first class infantry in the open since the Roman Emperor Crassus' defeat at the hands of Parthian horse archers in 53 BC. Today's rough equivalent would be—or would have been a decade ago—the seemingly impossible debut of radar-proof aircraft.

This was, in fact, the birth of modern infantry, shortly followed by the replacement of the *columna* with the larger tercio, the first permanent tactical and administrative military formation since the disappearance of the Roman legion.[14] It is difficult to overstate the importance of these developments. In the short term, they provided the wherewithal to halt the westward expansion of the Ottoman Turks.[15] In the long term, as Geoffrey Parker has persuasively argued in his seminal work, *The Military Revolution,*[16] the Spanish infantry of the 16th century were the inspiration and prototype for the soldiery of the 17th, 18th and 19th centuries that made European world dominion a reality.

The parallels with today's posited RMA are interesting. In both cases, existing technologies were exploited in new and innovative ways, gunpowder shoulder arms in the first instance and micro-miniaturized avionics and communications in the second. In both cases, the new acted in synergistic combination with the old when applied within a novel organizational and intellectual framework. One is tempted to draw parallels between the operational impact of low-observable strike platforms and that of the Spanish musket, and between that of F-16s and A-6s in DESERT STORM and Gonsalvo's *ginetes* after Cerignola! Might the operational impact of the concentration of tactical, administrative and logistical functions in the tercio be

likened to that of the STU-III scrambler telephone and secure fax machine half a millennium later?

Be that as it may, the Spanish "RMA" of the 16th century has a sobering epilogue. Spanish infantry retained its tactical dominance well into the 17th century, humbling the vaunted Swedish army—beneficiaries of yet another military revolution—at the battle of Nördlingen in 1634, but tactical brilliance did not preserve Spain from defeat in the Revolt of the Netherlands and strategic decline, a reality that bears reflection.

Setting aside for the moment the relationship between tactical superiority and strategic success, the 16th century Spanish RMA has further relevance to the issue of technological asymmetry. Shortly after their appearance, the new Spanish methods were unleashed against the Aztec and Inca empires in an extreme example of technological asymmetry—I would argue *the* extreme example of consequence in the modern era. Indeed, the Spaniards' enormous qualitative technological advantage and the seemingly impossible numerical odds against which they fought make this a limiting case for high tech/low end versus low tech/high end warfare. Although time and space permit only a brief synopsis, close examination of that case yields findings relevant to today's concerns. I have attached a more finely-grained analysis in an appendix.

Suffice it to say that raw technological superiority was vital to Spanish success, but not as a wonder weapon or "magic bullet." Rather technological advantage acted primarily as a facilitator, serving tactically to magnify the effect of Spanish cohesion in combat, and strategically as a device for opening up options that would otherwise have been foreclosed. This facilitating role was pivotal in providing the military leverage for the forging of alliances with Amerindian groups critical to Spanish success. The most important Spanish technologies were not the highest of high tech available, and all were interdependent in ways that varied according to geographic, topographical, and

cultural factors. Horses provided the Spanish with their most important single technological advantage, but did so within a tactical context established by steel swords and lance points.[17] One of the most important tactical benefits of horses was the effect of their speed on Amerindian security; charging cavalry were on occasion able to overrun pickets and reach the main body before news of their coming.

Conversely, horses placed significant constraints on Spanish operational and strategic mobility, for properly conditioned armies unencumbered by pack and draft animals moved more swiftly than those with horses.[18] While gunpowder was essential to Spanish success in Mexico, particularly in the siege of Tenochtitlan, it was superfluous in the Andes. The conquistadors made effective use of crossbows at a time when they had been entirely supplanted by gunpowder arms among Spanish infantry in Europe[19]; as with firearms, crossbows were more important in Mexico; the greater lethality of Mexia weaponry in hand-to-hand combat was the primary reason.[20]

Nor did all the technological advantages lie with the Spaniards. The Aztecs and Incas possessed important advantages in strategic communications and mobility, a product of their well-organized empires, and, in the Andean case, the remarkable Inca road network. Inca hosts, unhindered by pack animals, possessed unequaled strategic mobility.[21] Both Aztec and Inca possessed superior logistical systems, able to deliver weaponry, clothing, and rations, all suited to the environment, in quantity over considerable distances, an advantage effectively neutralized by the ability of the Spaniards' local allies to do the same. Both sides used terror, though the effects seem to have roughly canceled each other out.[22]

The most basic hypothesis to emerge from my limiting case study is that in even the most extreme case, technological asymmetry takes effect within a tactical, operational, and strategic context established and mediated by such basic factors as geography, topography, climate,

and culture. What works against one enemy might not against another for reasons having little to do with the degree of technological asymmetry. The next is that while extreme high tech superiority bestows clear tactical advantages, those advantages tend to assume strategic importance indirectly as enabling factors for operational and strategic advantage. The last is that human factors, both individual and collective, determine the degree to which technological advantage can be exploited and the manner in which it is done.

I will proceed by applying these hypotheses to selected modern cases, organized by degree and kind of asymmetry. My choices were impressionistic and highly selective, slanted toward cases that can inform U.S. about the kinds of opportunities and problems that I see arising from our current situation and toward cases where I believe I have something to say. I have deliberately slighted that category of conflict with which we are most fascinated and in which, historically, we have been most successful—that between high tech, high end opponents.

Beginning with gross high tech/low tech asymmetry with rough numerical parity, the closest we have to our limiting case is the British Zulu War of 1879 and concurrent pacification operations in the Sudan. These cases show striking similarities to those we have just examined, African steel spearheads balancing the effect of British repeating rifles. In both cases, superior African tactical mobility, and in the Zulu case strategic mobility, gave the British some nasty surprises, as did superior African exploitation of the terrain.[23] Ultimately, the overwhelming preponderance of British resources acted in combination with technological advantage and limited British objectives to permit the British to leave their former enemies chastened but essentially in place. The tactical lesson is that the lowest of low tech weapons used with panache by skilled and disciplined combatants on their home turf can be brutally effective. The strategic lesson is that low tech tactical brilliance is most unlikely to secure outright victory

over a determined high tech, high end opponent, but may act in combination with exogenous factors to produce something less than total defeat: the Zulus, after all, are still a major political factor in South Africa.

My next category is what I would term low tech, low end niche advantage, typically fielded by a minor power with limited resources. The classic example is the Boer War of 1899-1902, in which the Dutch farmers of South Africa armed with state-of-the-art bolt action magazine rifles inflicted a series of punishing defeats on British forces, inflicting some 2,000 casualties for a loss of just over 100 in a span of just five days, termed "Black Week" by a hysterical British press. The Boer advantage was not so much superior technology as superior training. British Lee Enfields were every bit as good as Boer Mausers and Mannlichers, but the Boers were able to deliver accurate fire against massed formations at 1,000 yards while the British were trained for traditional massed fire at shorter ranges. This is a particularly interesting example in that the Boers were anything but disciplined soldiers, suggesting that appropriate technology can on occasion compensate for shortcomings in discipline or even cohesion. The Boers were ultimately ground down by weight of numbers and resources, but the British learned from them the value of superior rifle marksmanship, a lesson applied with devastating effect during combat against the German Army in 1914. But the lessons that served the British so well in August and September of 1914 must be qualified, for the effectiveness of Boer marksmanship at extreme ranges was a product of the sparse vegetation and long hilltop vistas of South Africa. Ironically, the military topography of Europe was very different, and the range and power of Enfield, Mauser, Mannlicher, and American Springfield rifles were largely wasted there in both World Wars.

Low tech, low end niche advantage also applied in the Russo-Finnish Winter War of 1939-1940, when lightly-equipped Finns wreaked havoc on armored and mechanized Soviet units in the opening stages of the

conflict.[24] Familiarity with terrain and climate were pivotal to Finnish success, as was superior tactical skill and cohesion, but the advantages bestowed by such low tech items as winter clothing, snow shoes, and skis—plus the ability to use them—and the marvelously simple and reliable Suomi submachine gun, were vital as well.[25] Ultimately Soviet numbers and resources forced the Finns to sue for peace, but their effective resistance preserved Finland's independence. As with the Boer War, the lessons extracted from the conflict cast long shadows. Though I cannot establish an explicit link to the Winter War, Soviet armored forces were appreciably more effective by 1941, the shock of strategic and tactical surprise and initially incompetent leadership at the top notwithstanding. The Red Army proved to be infinitely better equipped for winter combat than the Wehrmacht. Might Hitler and the Wehrmacht have been so ready to attribute the Red Army's humiliation to Slavic racial inferiority as to remain uninformed about the Finns' subtle, but real advantages in the low tech, low end arena? That would certainly help to explain Hitler's sanguine expectations for Operation Barbarossa.

The same basic relationships apply to what I would term medium-tech, low end niche advantage. Examples include the Egyptian use of Soviet SS-9 Sagger wire-guided anti-tank missiles in the early stages of the 1973 Yom Kippur War and, arguably the use by the Afghan Mujaheddin against Soviet forces of British Blowpipe and U.S. Stinger shoulder-fired, heat-seeking anti-aircraft missiles in the recent Afghan war. In both cases, the weapon in question proved well-suited to the socio-psychological characteristics of the forces using them, redressing, at least temporarily, significant tactical liabilities. The use of Saggers to blunt the initial counterattack by Israeli armor against Egyptian forces that had breached the Suez Canal is the key datum. Note, however, that terrain was again a significant factor.

A further example involves the use of Soviet SA-7 "Grail" shoulder-fired, heat seeking missiles by North Vietnamese forces in the final stages of the Vietnam War, particularly in the 1975 Ho Chi Minh offensive. In this case, the effectiveness of the niche weapon was attributable not so much to the user-weapon fit as to the peculiar vulnerabilities of the armed forces of the Republic of Vietnam (ARVN). We had consciously declined to equip the South Vietnamese Air Force with first-line jet fighters, providing them instead with a mix of AC-119K side-firing gunships and AT-37s and F-5s, jet trainers converted to the attack role. Of the latter, the most effective was the comparatively slow twin-jet AT-37, on which the ARVN had become tactically dependent. The low speed that made the AT-37 an effective ground support aircraft rendered it highly vulnerable to the SA-7 (the lumbering piston-engined AC-119 was even more vulnerable, particularly in daylight), and the swift neutralization of a major component of the ARVN supporting weapons mix clearly accelerated the collapse of the South Vietnam forces. The lesson in all three examples is that a modest increment of technological advantage applied to the right operational niche can make a major difference tactically and, at least potentially, strategically. It is worth noting that in the AC-119K's sophisticated night vision, target acquisition, and fire control systems the ARVN had a high tech advantage that, because of the conditions of combat, proved strategically worthless.

When the low end niche advantage is high tech, the results can be even more telling, at least over the short term, even against a high tech, high end opponent, particularly when applied by surprise. My first reference here is to the impact of Syrian-operated, Soviet-supplied mobile anti-aircraft systems on the early stages of the 1973 Yom Kippur war, specifically the SA-6 radar-guided missile system and ZSU 23-4 radar and optically-fired gun system.[27] By way of background, by 1973 the Israeli air force had long since taken the measure of the Syrian air force,

partly due to superior American-designed aircraft and missile systems and partly—one might argue mostly—as a result of the superior quality of Israeli pilots and aircrew. I would add parenthetically that the Syrian qualitative disadvantage in the pilot arena was partly attributable to President Hafez al-Assad's insistence, for political reasons, on recruiting pilots heavily from the Alawi religious minority of which he is a member. The percentage of Alawis capable of becoming first rate fighter pilots is no doubt as high as that for any other comparable group, but since the Alawis are few in number quality inevitably suffered. Having earlier taken the measure of the Soviet SA-2 radar-guided missile, using tactics developed by U.S. forces over North Vietnam, the Israelis confidently launched their initial sorties against the attacking Syrian Army only to receive a shock that must have ranked close to that experienced by the first *macahuitl*-wielding Amerindians in taking on mounted Spaniards.[28] They had learned that they could handily out-maneuver the SA-2; they could not out-maneuver the SA-6.

In the absence of effective Israeli electronic countermeasures, the SA-6 proved lethal at high and medium altitudes, and attempts to underfly the SA-6 radars to attack tactical targets served only to demonstrate the ZSU 23-4's brutal effectiveness.[29] Israeli ground units defending the Golan had to do with minimal air support for the first critical days of the war, and the Israeli air force returned to the fray in force only after the Syrians had expended most of their missile reloads. One obvious lesson is that tactical complacency has no upside; another is that the unexpected, selective use of high tech weaponry has giant-killing potential. Another is that a polity that has difficulty producing skilled fighter pilots may well be able to field anti-aircraft missile crews with more than enough competence to make a significant operational difference.

A more equivocal example of low end/high tech niche advantage can be seen in the air war over North Vietnam, 1965-1972, in which the North Vietnamese made effective

use of a mixture of high and medium-tech radar, missile, gun, and fighter systems to exact a disproportionate toll on U.S. air forces. The net high tech advantage was clearly with the US, but the communists were able to effectively exploit restrictive American rules of engagement, the weather, and the tactical synergy achieved by the skillful employment of a dense radar warning and ground-Scontrolled intercept (GCI) net, radar-guided SA-2 missiles, anti-aircraft artillery, and manned interceptors.[30] One of the most interesting aspects of this case lies in the remarkably different institutional approaches adopted by the U.S. Air Force and Navy to address the problem of excessive aircraft losses and poor air-to-air exchange ratios over North Vietnam. Seemingly instinctively, the Air Force turned to almost purely technological solutions, developing sophisticated jamming, target acquisition, and warning devices while the Navy stuck with the same basic technologies and thoroughly revamped its air-to-air combat training program.[31] It was not quite so clear-cut as that, of course, for the Navy and Air Force shared many of the same technologies, notably the F-4 as a first-line fighter and AIM-7 and AIM-9 air-to-air missiles. They also shared the common goal of reducing aircrew losses, but the case provides an instructive lesson in the continuities of institutional mindset.

Fascinating as it is, I will cut short my discussion of the Vietnam air war, for it is not so clear-cut as the previous cases of technological asymmetry, if for no other reason than that the North Vietnamese possessed quantities of anti-aircraft artillery and SA-2 missiles such that to categorize their commitment as low end becomes misleading, shading over into conflict between high tech, high end opponents.

There is, however, a category of technological asymmetry involving high tech, high end opponents that deserves mention. That is the notion of surprise in the form of "wonder weapons" consciously designed to overcome a strategic disadvantage or override a debilitating

operational problem by pure technology. Almost by definition, high tech societies seeking to minimize the social and economic costs of war, of whom we are one, are particularly prone to pursue this option. Prominent recent examples include the German use of chlorine gas in early 1915[32]; the German use of sophisticated artillery preparations orchestrated by the famous Lieutenant Colonel Brüchmuller in conjunction with *Stoßtrupp* (shock troop) infiltration infantry tactics in 1917 and 1918[33]; the Japanese naval armaments program prior to World War II; the German V-2 program[34]; and the Manhattan Project. Of these, the Manhattan Project worked. The Manhattan Project represented a pinnacle of effective staff work, something at which we as a society are very good, at least when we let our military institutions take the lead.[35]

Of the cases cited above, the Manhattan Project aside, the most extreme and instructive example is the case of the Imperial Japanese Navy (IJN) which, looking forward to war with the United States and keenly aware of its gross high end inferiority, took unprecedented efforts to achieve high tech superiority across the board. These efforts, brilliantly laid out by Mark Peattie and David Evans in their recent book *Kaigun* —so central was this effort to the heart of the IJN that their title is the Japanese word for Navy—yielded just what was intended.[36] At the initiation of hostilities in December 1941, the Japanese Navy enjoyed major qualitative advantages in key performance factors in a remarkable number of key systems; the Zero carrier fighter, the Long Lance oxygen torpedo, torpedo-armed heavy cruisers, and the super battleships *Yamato* and *Musashi* are prominent examples. But the advantages, though very real tactically, proved illusory, for the resultant operational instrument was brittle. Instructively, the key vulnerability node was human. In their determination to wring the last iota of advantage from superior aircraft performance, the Japanese Navy embraced a training program so selective and so demanding that it proved incapable of providing the replacements needed to sustain

the war of attrition that was the inevitable result of faulty strategic appreciations. As in the 16th century, human factors count.

At least from our American perspective, then, the wonder weapon approach seems a chimera, but there were some near misses. Consider the V-2 program, generally derided as a gross waste of strategic resources, as indeed it was—as things turned out. From the German perspective, the Eastern Front was the critical front when the V-2 was operationally deployed in the summer of 1944, and the V-2 was utterly useless in the east.

But what if the Normandy invasion had been repulsed, as could easily have been the case? V-2s, fired from mobile launchers within easy reach of London and the English midlands, could have wrought havoc on the British war economy and forced the evacuation of London. Efforts to suppress the feeble V-2 offensive that, in fact, ensued were no more effective than the equivalent effort against Iraqi Scuds in the Gulf War. The lesson here is that we should be careful not to read too many comforting lessons into our recent past. Among the comforting lessons that we are wont to draw from the Gulf War are those involving our considerable success in minimizing the effects of friction, and here my case studies suggest the counter-intuitive finding that friction plays a relatively minor role in conflicts involving gross technological asymmetry. Both the conquistadors and the Amerindian empires did a marvelous job of minimizing friction, and the same point applies to the British and Zulus. Whether this is an artifact of my data set or an inherent characteristic of extreme technological asymmetry I cannot at this point say, but I would certainly not exclude the latter possibility.

Conversely, qualitative technological niche advantages would appear to be fertile breeding grounds for friction. That was certainly the case in the early stages of the Boer War and the 1939-1940 Russo-Finnish Winter War. The deleterious effects of friction on the South Vietnamese

forces in 1975 are self-evident as are the lessons to emerge from the friction-infested skies of North Vietnam. The point applies as well to the 1973 Yom Kippur War, where friction played a major role in driving the tempo and pace of operations, first to the detriment of the Israeli forces and then to that of the Syrians and Egyptians.

And so what are we to draw from all this? Is some high tech enemy likely to smack our *macahuitls* from our hands in an unanticipated high tech ambush? Are we likely to stub our high tech toes against some low tech rocks in the most miserable reaches of the Third World, or perhaps in our own back yard? Will clever enemies exploit chinks in our military armor with low tech, low end niche technologies, as they are surely attempting to do even as I speak?

I can offer some thoughts. As a nation, we Americans are very good at developing and deploying high tech systems, military as well as commercial. We are not so good at anticipating the cultural, geographic, and political circumstances under which they will be deployed and used. My note of caution extends not only, or even particularly, to the hardware, but mainly to the software, the human user and his or her live, breathing enemy. In assessing the problems and opportunities of technological asymmetry, we must not lose sight of the men and women who will use the high tech systems we prize so highly, nor should we be careless in anticipating where those systems will be used, for what tactical purpose, under what operational circumstances, and for what strategic objective.

In this context, pedestrian technologies and insights can be critical. Some years ago an American military pundit, probably an infantryman—I would love to take credit, but I can't—came up with an astonishingly effective law for predicting the location of our next major military commitment. I've been applying it for decades and it works beautifully. Closely examine our military footgear, then identify the country and climate for which it is least well suited, and that's where we're headed. We deployed to

Vietnam with leather combat boots beautifully suited to Western Europe; we deployed to the Persian Gulf with jungle boots tailored for the jungles of Southeast Asia.

Did I say high tech sneakers? Did I say crossbows, or the 21st century equivalent? What's today's strategic equivalent of a Suomi submachine gun or a MiG-17 over North Vietnam in 1972? Those, I am convinced, are key questions. If I were in a position of responsibility and could pull it off, I'd retain Hernando Cortés as a consultant, and Moctezuma as well. I might even look up the guy who ran North Vietnam's air defense system in the autumn of 1967, or even better his chief of staff and operations NCO.

APPENDIX

ASYMMETRICAL TECHNOLOGY AND THE SPANISH OVERTHROW OF THE AZTEC AND INCA EMPIRES, 1519-1539

From the historian's perspective, close analysis of the Spanish overthrow of the Aztec and Inca Empires offers important insights into the strengths and weaknesses of Amerindian political and social organization and belief structures. It also offers a significantly enhanced understanding of the wellsprings of Spanish military effectiveness at a time when the superiority of Spanish arms played a major role in world affairs. From the perspective of today's defense analyst or military professional, the exercise also suggests an approach for the analysis of the military impact of technological disparity in general, one that covers the analytical bases better than most. Precisely because the technological disparity was so great, pitting Chalcolithic[37] societies that lacked draft animals against combatants equipped with horses, steel weapons, and gunpowder, we are forced to consider causal factors that drop from the equation in less extreme cases or take effect so subtly as to be all but invisible.

Study of the overthrow of the Aztec and Inca empires also produces insights and conclusions, some of them counter-intuitive, that are relevant to today's concerns. For all the stark differences between the Spanish conquistador of the 16th century and his American equivalent of today or tomorrow, we are dealing with the same building blocks of military effectiveness at the cutting edge: the formulation and implementation of strategy; mobilization of resources, physical, fiscal and human; effectiveness in exploiting the capabilities and limitations of weapons systems; cohesion; and leadership. Perhaps most important, the Spanish,

Mexia, and Andean combatants put to the test in these encounters possessed the same basic physical and mental equipment as the combatants of today and tomorrow, with minor variations attributable to diet and, in the case of some Andeans, adaptation to the rarefied atmosphere of high elevations.[38] To be sure, there are enormous cultural differences between the two cases, but my main concern is with the technological difference between each and its putative enemy. I can do no more here than summarize salient observations and conclusions.[39]

Raw technological disparities on a weapon by weapon basis were not as important as is generally supposed in either Mexico or the Andes—forget the stereotypical notions of Indians fleeing in terror at the mere sight of horses and the discharge of firearms.[40] To be sure, the Spaniards amplified the psychological effects of tactical surprise with unexpected cannon blasts and by hanging bells from the necks of their charging horses,[41] but such devices were no different in theory or practice than the Luftwaffe's use of wind-driven sirens on Stuka dive bombers early in World War II; in both cases the novelty soon wore off.

Both Mexia and Andean military leaders quickly developed a sophisticated grasp of Spanish tactical strengths and weaknesses. The steepness of the tactical and technological gradient that they had to climb inhibited their ability to exploit their knowledge, but it is clear that a lack of perceptiveness and tactical agility within the means at their disposal were not among their problems. Significantly, their limitations were not individual, but collective. While individual Amerindian champions were capable of giving Spaniards a serious challenge on a one-for-one basis, the Spanish fought in mutually-supporting groups and rarely gave them the chance. Conversely, the Amerindians had no experience with fighting in disciplined mass formations and proved unable to make the socio-psychological adjustments that this kind of combat required before they were defeated.[42]

Recently-introduced European diseases played a role in eroding Amerindian morale in both cases, though a smaller one than is popularly supposed.[43] For all the terrors of epidemic smallpox in a virgin population, the Aztecs mounted a dogged defense of Tenochtitlan while battling smallpox and the Spanish at the same time.

Horses were essential to Spanish success, though within a tactical context shaped by the greater quickness and lethality of Spanish swords. A Spanish swordsman with his thin steel blade could strike with far greater quickness and lethality than his Amerindian opponents wielding a *macahuitl* (Mexia) or stone-headed club (Andeans), and swords were surely responsible for more Amerindian casualties than all other Spanish weapons combined, except perhaps in the siege of Tenochtitlan. But steel swords alone, however superior, could not have done the job, a point confirmed by the ease with which the Mexia repulsed the initial Spanish landings on the coast of Mexico, made without horses in 1517 and 1518.[44]

Tactical analysis clearly indicates that the speed, quickness, and flexibility of mounted shock action was the conquistadors' biggest single advantage in determining the pace and tempo of combat. In short, horses were more important than steel in determining the conditions under which combat was joined, enabling the Spaniards to engage and disengage at will. If we must choose between horses and steel, horses come first and it is worth noting that the older technology—by a millennium—was the more critical.[45]

Gunpowder was an indispensable ingredient of Spanish victory in the Valley of Mexico, but played a peripheral role in the Andes. Indeed, it is reasonable to argue that the conquest of Peru could have been achieved without gunpowder.[46] The difference between the Mexican and Andean cases is attributable to the Mexia's higher level of technological advancement, but only partly so.[47] The greater political and psychological robustness of the Aztec empire was an important factor as well. So too were the

political geography and military topography of the Valley of Mexico, where the fortified island city of Tenochtitlan posed difficult problems for the Spaniards. These forced Cortés to have small, cannon-armed warships built on the coast, disassembled, and brought inland to establish control over Lake Texcoco, cutting Tenochtitlan off from food supplies and reinforcement. The message here is that the advantages of technological "magic bullets" may well be mediated by the cultural and topographical peculiarities of the theater of operations.

As a subsidiary point, the crossbow played a significant role in both Mexico and the Andes at a time when, as noted in the body of the text, it had given way entirely to firearms among Spanish forces in Europe. As with firearms, the crossbow was more important in Mexico, clearly because the greater lethality of Mexia weapons in hand-to-hand combat placed a greater premium on keeping the Amerindian warriors at a distance. To put the point in perspective, the surprisingly high ratio of horses wounded to horses killed in combat in the Andes is testimony to the relative non-lethality of Andean weapons of close combat.[48]

The advantages of steel swords over stone-edged wooden *macahuitls* in Mexico and stone-headed clubs in the Andes were important, but the one essential ingredient to the conquistadors' success was cohesion in combat. Although the Amerindians quickly developed an accurate understanding of the advantages of Spanish weaponry, a generation was required for them to understand and begin to replicate the socio-psychological and tactical framework within which those weapons were employed. The key tactical problem was how to deal with a cavalry charge, and that required massed formations of disciplined pike-wielding infantry. Certain of the Andeans were stockpiling pikes in preparation for revolt within 25 years of the fall of the Inca Empire.[49] Though the rebellion was forestalled by aggressive Spanish action, it seems clear that the Andeans had grasped the socio-psychological essentials of the problem, for the pike, unlike traditional Andean

weapons, is effective only when used by disciplined masses of infantry.[50] Within a generation of the conquest, the Araucana Indians of southern Chile had mastered the full panoply of European warfare, including pike formations and mounted combat, and proceeded to fight the Europeans to a standstill, giving way only to demographic pressure that sedentary agrarian civilizations inevitably bring to bear on horse-nomad societies.[51] Finally, the conquistadors' technologically-derived tactical advantages were very real indeed and formed the cutting edge of conquest, but they would have gone for naught, as least in the short term, had Cortés, Pizarro, and their lieutenants not been superb diplomats, capable of forging effective coalitions with Amerindian allies.

There being no evidence that we have changed physiologically or in mental capacity since early Neolithic times, I would argue that findings like those above have relevance to the here and now. In other words, technological asymmetry affects war similarly regardless of time or place. That having been said, the single most significant conclusion to emerge from my 16th-century case study is that the dramatic asymmetry in weaponry, though a necessary condition for Spanish victory, was not a sufficient one, and that an understanding of the interplay among political, psycho-social, and technological considerations is needed to explain the conquistadors' success.

ENDNOTES

1. I am indebted to Dennis Showalter of Colorado College for having pointed out to me the usefulness of this distinction.

2. The logic behind my rank order generally follows that in Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report*, Washington, DC: U.S. Government Printing Office, 1993, Chapter 9, pp. 223-233, but broadens the focus to encompass ground and naval operations. Cohen was Gulf War Air Power Survey (GWAPS) Director; Keaney was the Summary Report Chief; I was Chief of Task Force II, Weapons, Tactics and Training.

3. I am indebted to Lieutenant Colonel Robert Eskridge, USAF; Lieutenant Colonel Charles Marshall, USAF; and Captain Jeffrey Hodgdon, USAF, of the GWAPS Weapons, Tactics and Training Task Force, for bringing this point to my attention. I initially scoffed at their inclusion of the color Xerox machine, but they convinced me of the enormous advantages in speed and accuracy in mission planning of dispensing with the need for every air crew to manually prepare its own strip map.

4. Such precision and confidence were, of course, a product of the ability to precisely establish geographic location to within meters.

5. In other words, the effects of low observability and the F-117A's night target acquisition, tracking, and designation capability were synergistic. Reflecting the value placed on its accurate bombing, F-117As flew only two percent of attack sorties in DESERT STORM, but struck 40 percent of strategic targets (Keaney and Cohen, p. 224). See also GWAPS, Vol. IV, *Weapons, Tactics and Training*, Washington, DC: U.S. Government Printing Office, 1993, henceforth *Weapons, Tactics and Training,* pp. 245-247.

6. Keaney and Cohen, *Summary Report*, pp. 223-233, rank aerial refueling third on their list of technologies that worked, behind low observables and LGBs and ahead of the HARM and STU-III scrambler telephone. Note, again, that their focus is on air operations.

7. Point made to the author by Colonel Bobby Buffkin, USAF, then Commandant of Red Flag, Nellis Air Force Base, Nevada, January 28, 1992; Buffkin's remarks were explicitly directed toward the lessons of DESERT STORM.

8. I use the term "antiquated" advisedly: the earliest Scuds were mounted on modified Joseph Stalin III heavy tank chasses of World War II vintage. For an analysis of the difficulty of combating the Scud menace from the air, see *Weapons, Tactics and Training*, pp. 274-295.

9. Charles Dunlap, *Weekly Standard,* January 29, 1996, pp. 22-28.

10. The exact quote is, "In the study of means, the critic must naturally frequently refer to military history, for in the art of war experience counts more than any amount of abstract truths," in Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, ed. and trans., Princeton: Princeton University Press, 1967, p. 164. See also p. 170 where Clausewitz notes that the performance of Napoleon's guard under fire would be inconceivable had not professional witnesses actually seen it.

11. See Andrés Mas Chao, "Cerignola, Bicocca et Pavia: L'arme à feu individuelle comme facteur décisif au combat," *Acta 22: XXII Kongress der Internationalen Kommission Für Militärgeschichte,* Heeresgeschichtliches Museum: Vienna, 1997, pp. 195-206, for an analysis of the impact of individual firearms in early Spanish victories over the French.

12. See Charles W. C. Oman, *A History of the Art of War in the 16th Century,* London: Meuthen and Company, 1937, pp. 53-54, who quotes the Italian condottiere Fabrizio Colonna's sarcastic remark that Gonsalvo's victory was due neither to the courage of the general nor the steadfastness of the troops, but to "a little ditch and a parapet of earth, and the arquebus."

13. The French captain François La Noue commented on the remarkable achievement of a body of 4,000 Spanish infantry that was forced to retreat by a force of some 18-20,000 Muslim cavalry in one of the Emperor Charles V's North African campaigns, probably that of 1535, and repelled dozens of charges, getting away with a loss of only 80 men and killing some 700 of the Muslims. Cited in Oman, *Sixteenth Century*, p. 44.

14. For a recent interpretation, see John F. Guilmartin, Jr., "Infantry Weapons," Robert Cowley and Geoffrey Parker, eds., *The Reader's Companion to Military History,* New York: Houghton Mifflin Company, 1996, pp. 220-222.

15. The basic text is still Oman, *History of the Art of War in the 16th Century*. *See* Book VII, "The Turkish Attack on Christendom (1520-1606)," pp. 607-770, esp. 666-684. For a more recent interpretation, see John F. Guilmartin, Jr., "The Military Revolution: Origins and First Tests Abroad," *The Military Revolution Debate: Readings on the Military Transformation of Early Modern Europe*, Clifford J. Rogers, ed., Boulder, CO: Westview Press, 1995 (henceforth *Origins)*, pp. 299-333, esp. pp. 318-322.

16. Subtitled *Military Innovation and the Rise of the West, 1500-1800*, Cambridge: Cambridge University Press, 1988.

17. See Appendix. The first Spanish expeditions to land forces on the Mexican mainland in 1517 and 1518, lacked horses and were handily driven off by the Mexia; see Bernal Díaz del Castillo, *The Discovery and Conquest of Mexico, 1517-1521*, Irving A. Leonard, trans., New York: Farrar, Strauss and Cudahy, 1956, pp. 3-28.

18. See note 21, below.

19. The first of the Spanish incursions onto the North American mainland that led to the conquest of Mexico was in 1517, and the final Inca resistance was quelled by 1539. Gonsalvo de Cordova's force that landed in Italy in 1495 fielded crossbows and *escopetas*, precursors to the arquebus, in roughly equal numbers. By the battle of Ravenna in 1512, the arquebus had entirely replaced the crossbow, and there is some evidence that the larger and more powerful musket was in use. See Oman, *16th Century*, pp. 130-149.

20. This is my reading of the evidence based on the sources cited in the appendix, particularly Bernal Díaz del Castillo, *Discovery and Conquest*, cited above. The key Mexia weapon was the *macahuitl*, a wooden sword shaped like an oversized cricket bat with razor-sharp obsidian edges. Though the obsidian was brittle and shattered on impact with steel, it was a slashing weapon of awesome effectiveness. By contrast, the Andeans depended primarily on stone-headed clubs and, to a lesser extent, spears.

21. See John F. Guilmartin, Jr., "The Cutting Edge: An Analysis of the Spanish Invasion and Overthrow of the Inca Empire, 1532-1539," *Transatlantic Encounters: Europeans and Andeans in the 16th Century*, Kenneth J. Andrien and Rolena Adorno, eds., Berkeley: University of California Press, 1991 (henceforth *Cutting Edge*), p. 48, for the speed of Inca armies; a network of warehouses stockpiled with weapons, clothing, and rations, including desiccated tubers and meat, were a significant contributing factor. For an analysis of the negative effect of pack and draft animals on the mobility of armies in the pre-modern era, see Donald W. Engels, *Alexander the Great and the Logistics of the Macedonian Army*, Berkeley: University of California Press, 1978, pp. 20-23.

22. The Aztecs, by forcing captives to dance before their idols within view and hearing of the Spaniards during the siege of Tenochtitlan, then ripping the captives' hearts out and tumbling the bodies down the temple steps; and the Spaniards in Peru by cutting off the right hands of captives, then releasing them to spread demoralization, and by executing women used as porters. Both Amerindians and Spaniards used torture routinely.

23. Zulu victory at Isandlwana, January 22, 1979, was balanced by defeat at Rorke's Drift 2 days later. Rudyard Kipling's poem "Fuzzy Wuzzy" provides eloquent testimony to the effectiveness of the Sudanese.

24. Allen F. Chew, *The White Death: The Epic of the Soviet-Finnish Winter War*, East Lansing: Michigan State University Press, 1971, pp. 6-30, 97-125.

25. The Suomi's simple and reliable blowback action was widely imitated not least of all by the Soviets. See Ian Hogg and John Weeks, *Military Small Arms of the Twentieth Century*, Chicago: Follett Publishing, 1973, pp. 2.10-2.11.

26. The author, then an Air Force major flying HH-53 rescue helicopters, tracked the final stages of this process though daily intelligence bulletins while aboard USS *Midway* awaiting the order to execute Operation FREQUENT WIND, the evacuation of Saigon.

27. Chaim Herzog, *The War of Atonement, October 1973*, Boston: Little Brown, 1975, pp. 78-95, esp. p. 87, and pp. 188-191.

28. The *Macahuitl* was a wooden broadsword resembling an oversized cricket bat with razor-sharp obsidian edges. It had awesome power as a slashing weapon; but the edges were brittle, and it required a time-consuming swing. The Spanish swordsmen could slash far more quickly and had the option of thrusting.

29. Christopher Campbell, *Air Warfare: The Fourth Generation*, New York: Arco Publishing, 1984, pp. 100-101.

30. See Marshall L. Michel III, *Clashes: Air Combat over North Vietnam 1965-1972*, Annapolis, MD: Naval Institute Press, 1997, for the first comprehensive look at the air war "Up North."

31.This is a major theme in Michel, *Clashes*, but see particularly Chapter 9.

32. Charles E. Heller, *Chemical Warfare in World War I: The American Experience, 1917-1918*, Leavenworth, KS: Papers No. 10, Fort Leavenworth, KS: Combat Studies Institute, September 1984, pp. 4-12.

33. Bruce I. Gudmundson, *On Artillery*, Westport: Praeger, 1993, pp. 87-106; Timothy T. Lupfer, *The Dynamics of Doctrine: The Changes in German Tactical Doctrine During the First World War*, Leavenworth Papers No. 4, Fort Leavenworth, KS: Combat Studies Institute, July 1981, pp. 3-49.

34. Michael J. Neufeld, *The Rocket and the Reich: Peenemünde and the Coming of the Ballistic Missile Era*, New York: The Free Press, 1995, pp. 272-275.

35. Private communication from Daniel Jacobowitz in response to an early draft of this paper.

36. Mark R. Peattie and David C. Evans, *Kaigun: Strategy, Tactics and Technology in the Imperial Japanese Navy 1887-1941*, Annapolis, MD: Naval Institute Press, 1997.

37. Chalcolithic societies possess the ability to smelt precious metals and copper, but rely on stone implements for cutting and grinding.

38. Bernal Díaz del Castillo, *The Discovery and Conquest of Mexico, 1517-1521*, Irving A. Leonard, trans., New York: Farrar, Strauss and Cudahy, 1956, pp. 5-16, discusses the 1517 Cordova expedition's clashes with Mexia warriors at several points along the Campeche coast and a subsequent clash in Florida with North American forest Indians. Díaz describes the latter as "very big men" in implicit contrast to the former. The Mexia had no domesticated meat-producing animals aside from small hairless dogs and subsisted primarily on maize, with beans as their only significant source of dietary protein. Mexican conscripts of the 1830s and 1840s, raised on the same basic diet, were extremely short, and enlisted men less than five feet tall were common. See *El Soldado Mexicano, 1837-1874*, Mexico City: Edícíones Nieto, Brown Hefter, 1958, p. 4. Certain Andean tribal groups had lived at extremely high altitudes for enough generations to be the beneficiaries of genetic selection in favor of increased lung capacity, and warriors from these groups were selectively recruited by the Incas for use at high altitudes.

39. For in-depth analysis of the Andean case, see John F. Guilmartin, Jr., "The Cutting Edge: An Analysis of the Spanish Invasion and Overthrow of the Inca Empire, 1532-1539," *Transatlantic Encounters: Europeans and Andeans in the 16th Century*, Kenneth J. Andrien and Rolena Adorno, eds., Berkeley: University of California Press, 1991, pp. 40-69 (henceforth *Cutting Edge*). For an overview of both cases, see Guilmartin "The Military Revolution: Origins and First Tests Abroad," Clifford J. Rogers, ed., *The Military Revolution Debate: Readings on the Military Transformation of Early Modern Europe*, Boulder, CO: Westview Press, 1995, pp. 299-333, esp. pp. 308-313 (henceforth *Origins*).

40. Mexia champions proved remarkably effective, even against mounted Spaniards, on a one-on-one basis, but, unless surprised, the Spanish engaged the Amerindians in mutually supporting groups. In the first encounter in the Andes, the ambush of the Emperor Atahualpa's bodyguard by Francisco Pizarro's men at Cajamarca in 1532, the Incas fought with stoic bravery against the full array of Spanish weapons and were butchered in the thousands.

41. *Cutting Edge*, p. 56, n. 58.

42. Interestingly, the contemporary Ottoman Turks, who in other ways were on a technological par with the Spanish, were unable to make the shift either. See *Origins*, pp. 313 ff.

43. Francis J. Brooks, "Revising the Conquest of Mexico: Smallpox, Sources and Population," *The Journal of Interdisciplinary History*, Vol. XXIV, No. 1, Summer 1993, pp. 6-7. Brooks argues, persuasively in my view, that exaggerated descriptions of the effects of smallpox were the product of apocalyptic sermons by Franciscan friars emphasizing the helplessness of the heathen in the face of God's wrath.

44. These were the Cordova and Grijalva expeditions; Bernal Diaz del Castillo, cited above, is the basic source.

45. This is a modification of my conclusions in "The Cutting Edge," where I listed steel swords first. Both conquistadors and Amerindians were fully aware of the importance of horses, the former treating their mounts almost as partners in the enterprise, and the latter going to great lengths to kill them. Horses were first domesticated for war around 2000 BC; steel weapons did not begin to appear until around 1000 BC.

46. *Cutting Edge*, p. 57.

47. Most basically, the Mexia civilization was literate, while the Andean was not. The Mexia technology of war was generally superior to that of the Andeans, who fought primarily with stone-headed clubs and had no equivalent of the slashing *macahuitl*. Organizationally, the two civilizations were on a rough par, though the extreme centralization of the Inca state was a major liability. Unlike the Mexia, the Andeans smelted bronze, but only in small quantities and did not use it for weapons.

48. *Cutting Edge*, p. 52. This was particularly evident at the battle of Vilcaconga in 1533, the first encounter between an Inca army and conquistadors in the open field. The Incas caught the Spanish vanguard in a perfect ambush, charging downhill on the conquistadors at the end of a long day's march just as dusk fell; they killed eight horses and wounded another dozen or so, but were unable to annihilate the Spaniards despite a huge numerical advantage. *Cutting Edge*, p. 57.

49. *Ibid.*, p. 61.

50. *Ibid*.

51. *Ibid*., n. 75.

MYTH OF THE *BLITZKRIEG*

Robert A. Doughty

Numerous battles have occurred in the 20th century, but perhaps no other military operation has had a greater influence upon our perceptions of war in this century than the 1940 campaign in which the Germans defeated the French. Whether in broad political and sociological analyses seeking to examine war in general or in more narrow polemics aiming to convince readers or decisionmakers, analysts and historians have often used the example of the 1940 campaign to hammer home their points or portray their ideas about military strategy or operations. In recent years, the example of the 1940 campaign has been particularly evident in publications pertaining to the so-called "Revolution in Military Affairs." Its theorists have argued frequently that a dramatic change in warfare occurred between 1918 and 1939 and have used the example of this change to suggest a model for the future. Some have insisted that Germany exploited the technological opportunities more readily than the Western democracies.[1] Others have associated *Blitzkrieg* with a "RMA" because of "tactical, operational, conceptual, [and] organizational" advances.[2] Still others have seen *Blitzkrieg* emerging from a combination of technological and conceptual advances;[3] and a few have argued that the Germans developed *Blitzkrieg* because they recognized they could not win a war with their existing military capabilities.[4] Whatever the theorists' explanation—the unleashing of a new way of war, the disintegration and defeat of a major power, or the apparently decisive role of new technologies—aircraft and tank often fit nicely into their explanations or models of how the waging of war can change swiftly and affect dramatically the destiny of world powers.

Despite the wealth of information about *Blitzkrieg*, much of our common knowledge pertaining to the 1940

campaign and to the concept of a *Blitzkrieg* is pure myth. "[A]s an operational design," Michael Geyer has said, "it was a make-believe spectacle that was put together in hindsight for public consumption."[5] Sam Lewis has added, "Contrary to popular belief, there was no '*Blitzkrieg* Era' in the history of the German Army."[6] In reality, the 1940 campaign had more modest goals than the swift, overwhelmingly decisive victory the Germans achieved. Though the Germans entered battle in May 1940 hoping for a quick victory, they had no expectations of a *Blitzkrieg*-like campaign and ultimately owed their success to the favorable outcome of several encounters won only by slim margins. Moreover, they owed much of their success to the infantry, not the tank or aircraft, and achieved victory by relying more on traditional aspects of tactics, operations, strategy, and leadership than on any revolutionary new ones. The crushing nature of the victory nonetheless enabled the Germans to manufacture and advertise for political and military purposes a "make-believe spectacle" that bore little resemblance to their actual experience. Ironically, the Germans fell victim to their own myth when they failed to examine rigorously the 1940 campaign and invaded the Soviet Union in June 1941 expecting to replicate their relatively easy victory over the French.

The myth of the *Blitzkrieg* begins with misconceptions about the origins of the term.[7] For some time historians have believed the term came from an article published in *Time* magazine about the time of Poland's fall in which Commander-in-Chief of the Army General Walther von Brauchitsch was tagged a "Blitzkrieger" and the "Lord of the Lightning."[8] William J. Fanning, Jr., recently demonstrated in an article in *War & Society*, however, that the word "*Blitzkrieg*" appeared occasionally between 1936 and 1937 and stemmed from the widespread use—in several languages—of the term "lightning" to describe the speed and power of modern armies in the late 1930s.[9] European officials and analysts often used the term "lightning" during that decade to describe the "knockout blow" favored after

the dreadful experience of the long total war from 1914 to 1918.[10] In German publications, for example, writers sometimes used such words as *Blitzartig* (lightning-like), *Blitzfunken* (lightning sparks), or *Blitzschlag* (lightning blow). Though the Germans used the term *Blitzkrieg*, they used it infrequently and associated it primarily with the concept of a short war.[11]

Despite significant interest in avoiding a long war, no theorist linked the word "*Blitzkrieg*" to a quick, knockout blow with closely coordinated tank and air forces. What the Germans did instead was develop advanced concepts for mobile warfare, many of which provided the foundation for the successful 1940 campaign. As James Corum has demonstrated, the Germans, led by General Hans von Seeckt, conducted a careful and rigorous analysis of their experiences in World War I and used the results of this assessment as the foundation for their efforts to develop methods and equipment for mobile warfare in the interwar period.[12] When the Panzer division appeared in 1935, its creation was, as Corum has observed, less a revolutionary step than a "natural evolution" from the methods developed in World War I and the 1920s.[13] Moreover, though Guderian was a leader in the development of armored warfare, he was not alone in an oasis of ignorance and conservatism.[14] A lively debate occurred in German military literature in the 1930s over the role of armored and air forces, and the General Staff was well aware of the opportunities afforded by the tank and airplane. In reality, the inadequacy of the German economy and the consequences of Hitler's rapid expansion in the late 1930s retarded or disrupted the development of motorized and mechanized forces more than the conservatism of the German military.[15]

Even the notion of General Erich von Manstein's selling to Hitler the idea of a *Blitzkrieg* across France fades when examined carefully, as does the notion of Hitler's having developed almost by himself the strategy and tactics enabling the Germans to race across France.[16] Though Manstein started flooding the headquarters of Chief of the

General Staff General Franz Halder in late October 1939 with self-serving suggestions for Marshal Karl von Rundstedt's Army Group A, of which he was Chief of Staff, to make the main attack,[17] Hitler had asked about the possibility of attacking through the Ardennes long before he learned of Manstein's proposal.[18] Despite Hitler's interest, an energetic assessment of an offensive through the Ardennes did not begin in earnest until the French obtained portions of the German plan from a downed German aircraft in Belgium on January 10, 1940,[19] and preparations for such an offensive began only after extensive war games revealed the strategic possibilities.[20]

In the final analysis, German strategy in May 1940 emerged after a long and careful assessment and planning effort, not from a prophet of armor convincing Hitler at a dinner party to seek a breakthrough at Sedan.[21] The combination of Hitler's dabbling in questions of military strategy and operations, Brauchitsch's and Halder's doubts about trying a variant of the disastrous Schlieffen Plan, Rundstedt's and Manstein's seeking a more ambitious role for their army group, and France's serendipitously obtaining a copy of the earlier draft of *Fall Gelb*—led the Germans to choose the risky solution of attacking through the Ardennes.[22] And their choice was based more on considerations of strategic and operational possibilities than on notions of a new method of warfare or on the outcome of a cautious, step-by-step staff assessment. As Karl Frieser has observed, the campaign ultimately was "an operational act of desperation to get out of an unfavorable strategic situation."[23]The 1940 campaign also bears little resemblance to the jaunty gallop across France sometimes suggested by historians, particularly in the years immediately following World War II.[24] The experience of XIXth Panzer Corps illustrates this clearly. Beginning on the first day of the attack, May 10, the Germans encountered unexpectedly strong resistance from 2nd Battalion, 1st Regiment of the Belgian *Chasseurs Ardennais*. A light infantry force relying on bicycles as its

main means of transportation, this battalion occupied the area around Martelange and Bodange on the border between Belgium and Luxembourg. On the first day of the campaign the combination of difficult terrain and some particularly valiant resistance from one *Chasseurs Ardennais* company at Bodange delayed 1st Panzer Division and placed the entire campaign at risk.[25]

Though *Guderian's XIXth Panzer Corps* subsequently raced across Belgium and encountered little resistance from the French, the Germans confronted numerous difficulties when they attempted to cross the Meuse River at Sedan. With the French defending with hardly more than two regiments along the river where XIXth Corps crossed, only one of the six main German crossings met immediate success, and one other managed to get sizeable forces over the river only after several attempts. Both of these crossings occurred in 1st Panzer Division's sector.[26] As for 2nd Panzer Division to the west of Sedan, both its crossings failed; its infantry managed to get across the river only after soldiers from 1st Panzer Division cleared the river bank on the far side.[27] As for 10th Panzer Division east of Sedan, both its crossings were stymied, but two squads, one led by a German engineer staff sergeant, succeeded in getting across and then carving out a small bridgehead against more numerous French forces.[28] Were it not for the remarkable success of these two squads, as well as that of Lieutenant Colonel Hermann Balck's 1st Infantry Regiment of 1st Panzer Division, the course of the entire campaign would have been substantially different. The French rushed large reinforcements to the threatened Sedan sector, and the loss of only one day in the pace of the campaign could have spelled disaster, but not necessarily defeat for the Germans. While the Germans probably would have achieved victory, they may have lost many more lives before XIXth Panzer Corps established a bridgehead south of the Meuse River.

Subsequent portions of the campaign also bear little resemblance to the popular notion of a jaunt across France. On the morning of May 14, for example, the Germans had

few tanks across the Meuse at daylight. Guderian's three panzer divisions had managed to complete only one bridge across the river during the night, and movement of tanks to the bridge proved difficult. The 2nd Panzer Regiment, the first tank unit to cross the Meuse, did not complete its crossing until 0800 hours. Prior to these tanks crossing the Meuse, an antitank company—accompanied by an engineer battalion—acted as the spearhead of the XIXth Corps' attack.[29] Similarly, a particularly interesting action bearing no resemblance to the common perception of the campaign occurred on May 15 at Chagny when a single French rifle company, reinforced by horse cavalry and several antitank guns, turned back an assault by the bulk of the tanks of 1st Panzer Division. The Germans had unwisely separated their tanks and infantry, and while Balck's 1st Infantry Regiment fought against fierce French resistance at La Horgne, the German tanks found themselves unable to push through French infantry on the heights above Chagny, 20 kilometers southwest of Sedan. The Germans succeeded in breaking through French defenders only after Balck's infantry pushed through La Horgne, advanced toward Chagny, and threatened the defenders' rear.[30] Much like the encounters at Bodange and along the Meuse, the encounter at Chagny turned in the Germans' favor because of their infantry, not because of their tanks. Beyond a doubt, the Germans owed their success at Sedan more to Balck's 1st Infantry Regiment than to any other unit. In short, the tanks were important, but without key support from the infantry, their accomplishments would have been much more problematic.

Airpower also played a role different than that commonly credited to it, particularly by those believing German aircraft functioned as "flying artillery."[31] In addition to gaining and maintaining air superiority throughout the campaign,[32] the *Luftwaffe* played a particularly important role early in the campaign when it maintained an impermeable umbrella over German columns advancing across eastern Belgium and when its

attacks across Northern France confused French military leaders about the location of the enemy's main attack.[33] The *Luftwaffe* also provided crucial support to German infantry on May 13 during the assault across the Meuse. In particular, the famous provision of limited air support for an extended period on the morning of May 13, rather than heavy support for a brief period, eroded the French infantry's will to fight and contributed significantly to the collapse of the French 55th Division, Guderian's main opponent along the Meuse.[34]

Though these contributions were important, German airpower did not prevent the French from reinforcing the threatened Sedan sector and destroyed very little on the ground. Despite the French High Command's slow recognition of the threat along the Meuse, they succeeded in moving 2nd Armored, 3rd Armored, 3rd Motorized, 14th Infantry, 36th Infantry, 53rd Infantry, 71st Infantry, 1st Colonial, and 2nd Light Cavalry divisions, as well as numerous artillery units, into the expanding breach. Second Army reported only two tanks destroyed by German aircraft.[35] Adding to the negative side of the column, the accidental killing by German air of the commanders of the German 1st Armored Brigade and 43rd Assault Engineer Battalion demonstrates the tenuous link between German air and ground forces. In short, German ground forces could not have succeeded without air support, but the *Luftwaffe* was hardly the decisive factor in the campaign,[36] and its contributions did not mark the opening of a new age in the history of warfare.

The hazardous and fragile nature of the campaign was reflected in the nervousness of the German High Command, particularly of Hitler. In an attempt to avoid interference from Berlin, Guderian's superior, General Ewald von Kleist, was less than forthright with his superiors and did not inform them fully of the meager number of German forces across the river late on May 13, the first day of the crossing. Instead, he reported to Army Group A that all three of Guderian's divisions had crossed the Meuse River

and that sizeable forces would cross the Ardennes Canal the following day. Since his message omitted any mention of the difficulties encountered by 2nd and 10th Panzer divisions, his superiors were unaware of the vulnerability of the German bridgehead near Sedan.[37] Despite von Kleist's having painted a more optimistic picture than the situation merited, the German High Command remained extremely nervous. On May 17, General Franz Halder, the Chief of the German General Staff, observed in his diary, "Rather unpleasant day. The Fuhrer is terribly nervous. Frightened by his own success, he is afraid to take any chance and so would rather pull the reins on us."[38] The following day Halder recorded in his diary, "The Fuhrer unaccountably keeps worrying about the south flank. He rages and screams that we are on the best way to ruin the whole campaign and that we are leading up to a defeat."[39] By May 19, however, Halder could record in his diary, "I am certain of success."[40] Though Hitler later acknowledged his concern about the French repeating the 1914 miracle of the Marne,[41] neither he nor virtually anyone around him expected such a rapid and easy victory.

Perhaps more than anyone else, Guderian recognized the slim margin by which the Germans had succeeded. In his memoirs he describes his visit to the heights overlooking the Meuse River on May 14 and his surprise that French long-range artillery had not caused larger German losses. He wrote, "At this moment, as I looked at the ground we had come over, the success of our attack struck me almost as a miracle."[42] In addition to having favorable luck, the Germans won because of their better doctrine and leadership and because of their ability to concentrate overwhelming combat power at the decisive point. Additionally, as James Corum has noted, "superior training" gave the Germans an important advantage.[43] In essence, the Germans outfought the French tactically and outsmarted them strategically, but their victory stemmed as much from French weaknesses as from German strengths. French doctrine was inadequate for the mobile

fighting Germany thrust upon them in May 1940, and French strategy was particularly vulnerable to a thrust to the Ardennes.[44]

Despite Guderian's realistic assessment, neither Guderian nor other German leaders subsequently acted as if the 1940 campaign were "almost a miracle." Ironically, the Germans themselves fell victim to the myths surrounding the campaign and to their own propaganda about the effectiveness of the *Blitzkrieg*. Instead of acknowledging the slim margin of their victory, the military concluded that they had accomplished something extraordinary against France and that they had begun the campaign with the intention of winning victory through what became known as a *Blitzkrieg*. As Michael Geyer has observed, "[T]he officers got their ideas about the new 'strategy' where everybody else got them as well. They saw themselves in the newsreels and in the movies doing the right thing."[45] Thus, myth outweighed reason, and the Germans confidently expected the whole world to share their unshakable faith in their invincibility and in the *Blitzkrieg*.

With regard to the influence of the 1940 *Blitzkrieg* on German thinking, Hitler had his eyes on eastern Europe long before he ordered his armed forces to begin preparations for an attack.[46] In his first meeting with the senior leaders of the German military only days after he first came to power, Hitler emphasized his intention to build up the armed forces and, after decrying Germany's insufficient room, declared his intention to use the resurrected armed forces to conquer "new living space in the East."[47] At a meeting on May 23, 1939, with several senior military leaders including General Wilhelm Keitel and General Franz Halder,[48] Hitler emphasized obtaining living space in the East, securing food supplies, and solving the problems of the Baltic Sea and states.[49] In other meetings with senior military officials on August 22 and November 23, 1939, Hitler again revealed his intentions to move east.[50] In the latter presentation, he addressed the question of a multi-front or two-front war, emphasizing that

Germany could engage Russia only when it was "free in the West."[51] An invasion of the Soviet Union was thus an essential part of Hitler's quest to rule Europe and his plan to gain new room in the East. As one German officer, however, later wrote, "The real background to his decision undoubtedly lay in his permanent, deep-rooted, and deadly hatred of Bolshevism."[52] Consequently, the capability to launch a *Blitzkrieg* attack was not what convinced Hitler to charge eastward; instead, the capability only added to his confidence and encouraged him to launch such an attack earlier than he might otherwise have done so.

Though the precise steps in Hitler's thinking remain uncertain, he apparently made the decision in late July 1940—barely a month after the defeat of France—to invade the Soviet Union. An important step in his decision-making process occurred on July 19, 1940, when he addressed the Reichstag in what the German propaganda machine called "An Appeal for Peace."[53] Preceded on the previous day by a victory parade through the Brandenburg Gate, an event of enormous propagandistic and political significance, Hitler assembled the senior officials of the Third Reich and showered the leaders of the 1940 campaign with praise and promotions.[54] In his memoirs Keitel described the "memorable" July 19 session in glowing terms, observing "Never before and never again were the generals of the German armed forces represented in such strength on the rostrum."[55] William Shirer, who attended the presentation as a foreign correspondent, noted in his diary,

> It is not to be a *Blitzkrieg* against Britain. At least not yet. In the Reichstag tonight, Hitler "offered" peace. He said he saw no reason why this war should go on.[56]

After the assembly, one German officer shouted to Shirer, "Can you make it out? Can you understand those British fools? To turn down peace now?" The officer concluded, "They're crazy."[57] Despite the staged performance at the Reichstag and despite the release of much movie footage showing tanks charging across Belgium and France,

Winston Churchill and the British refused to yield. Halder observed in his diary, "The Fuhrer is greatly puzzled by Britain's persistent unwillingness to make peace."[58]

As the probability of an invasion of Britain decreased in the weeks after the fall of France, Hitler's interest in attacking east increased. On July 22, one month after the fall of France, Halder recorded in his diary a summary of a meeting with Brauchitsch, who had met with Hitler the previous day. According to Halder, the Fuhrer believed that "Britain's position is hopeless. The war is won by us." Crossing the Channel, however, appeared "very hazardous" to him.[59] An invasion would occur only if Germany had no other way of dealing with Britain, and Halder expected Hitler to decide within a week whether the planned invasion would occur.[60] "Our attention," Halder wrote in his diary, "must be turned to tackling the Russian problem and prepare planning." In a reflection of his confidence in the *Blitzkrieg*, Halder noted that the objective in an operation against the Soviets would be to "crush [the] Russian Army or slice as much Russian territory as is necessary to bar enemy air raids on Berlin and Silesian industries."[61] Halder had begun preliminary preparations for such an operation as early as July 3,[62] and by July 27 his staff presented him the outline of their study of operational possibilities in the East.[63] Halder observed in his diary, "Total strength required 100 Divs."[64] Almost simultaneously a memorandum from the Navy revealed the difficulties of transporting troops across the English Channel, and Halder observed, "[W]e can throw away the whole plan of an invasion [of Britain]."[65]

Meanwhile, Hitler had decided to invade the Soviet Union and had informed General Alfred Jodl, Chief of Operations in the Armed Forces High Command (OKW), on July 29.[66] That same day Jodl revealed Hitler's intentions to a few officers of the OKW. While sitting in a train station near Berchtesgaden, Jodl first ensured the windows and doors were closed and then told his compatriots that Hitler had decided to launch a surprise attack against the

Soviets.[67] Two days later, July 31, Hitler addressed this important issue more formally with Germany's senior military leaders. Halder's diary summarized Hitler's main point:

> With Russia smashed, Britain's last hope would be shattered. Germany then will be master of Europe and the Balkans. Decision: Russia's destruction must therefore be made a part of this struggle. Spring 41. The sooner Russia is crushed, the better. Attack achieves its purpose only if Russian State can be shattered to its roots with one blow.[68]

Clearly, Hitler as well as Halder expected that "one blow" to come from another *Blitzkrieg*. Prior to the crucial days at the end of July, Hitler's great confidence led him to boast, "Now we have shown what we are capable of [doing]. . . . [A] campaign against Russia would be like a child's game in a sandbox by comparison [to the campaign against France]."[69]

Hitler's decision by no means was set in concrete on July 31.[70] Directive Number 12, which formally initiated preparations for a war against the Soviet Union, was not published until December 18. Meanwhile, the Army High Command (OKH) and OKW staffs worked separately to analyze strategic and operational alternatives for a campaign against the Soviets. Following some preliminary work by the operations section of the general staff, Major General Erich Marcks, Chief of Staff of 18th Army, worked alone—beginning in late July—to analyze the prospects of an Eastern campaign.[71] While the OKH and general staff conducted their planning, the OKW also prepared a plan. Under the direction of General Walter Warlimont, Section "L" (*Landesverteidigung*) of the Operations Department almost simultaneously completed a plan that became known by the name of its main author, Lieutenant Colonel Bernhard von Lossberg, as the "Lossberg study."[72] Then, on September 3, Major General Friedrich Paulus was ordered by General Halder to prepare another study—without reference to the other ongoing studies—of operational possibilities in the East.[73] Though the recommendations of

these studies varied considerably, all assumed the Wehrmacht was far superior to the Soviet Army, and none evinced any doubts about a German victory in a short, swift campaign.

Throughout the fall of 1940, the concept of a *Blitzkrieg* dominated planning and preparations even though the Germans rarely used the term. Marcks' study noted, "As in Poland and the West, success must be sought by means of surprise and speed. The conduct of operations is so conceived that in all armies mobile formations in the first wave will break through the Russian troops in front of the river and forest defenses and, supported by the *Luftwaffe*, continue the advance to seize corridors through the forests and river crossings."[74] Similarly, Lossberg's study asserted,

> The aim of a campaign against Soviet Russia is to destroy the mass of the Soviet Army in western Russia, to prevent the withdrawal of battleworthy elements into the depth of Russia, and then, having cut western Russia off from the seas, to advance to a line which will place the most important part of Russia in our hands and on which it will be easy to form a shield against Asiatic Russia.[75]

Hitler's Directive No. 21 on December 18 stated, "The German Armed Forces must be ready to crush Soviet Russia in a rapid campaign, even before the termination of the war with Britain. . . ." The directive added,

> The bulk of the Russian Army deployed in Western Russia is to be destroyed in daring operations with deep penetrations of tank spearheads; no [enemy] units should be permitted to remain intact and retreat into the wide Russian spaces.[76]

According to Karl Frieser, German confidence in the *Blitzkrieg* led them to seek a "super Cannae" in Russia.[77] Though Brauchitsch and Halder believed Germany should defeat Britain before turning east, both nevertheless believed victory against the Soviets could be achieved in a relatively short campaign.[78] In the July 22 meeting between Brauchitsch and Halder, the two generals agreed that

80-100 German divisions could easily defeat the 50-75 "good" Russian divisions[79] out of the 147 they expected to encounter.[80] Rejecting the notion of anything other than a relatively brief, intense war, they expected to avoid the failures of World War I and the demands, which Germany could not meet, of a long total war. In avoiding a long war, the Germans hoped to avoid a massive mobilization of their economy. Though Alan S. Milward's notion of a "*Blitzkrieg* economy"[81] exaggerates the connection between military and economic planning,[82] production of goods for the civilian economy nonetheless continued at a remarkably high level as the Germans dawdled at initiating economic preparations for the terrible demands they were about to encounter.[83] Failing to recognize completely the huge increase in scale required for a war against the Soviet Union, the Germans also failed to prepare logistically for a demanding campaign in the vast area of Russia. Here, too, assumptions of a short campaign—from 9 to 17 weeks[84]—overruled special measures in obtaining, transporting, or accumulating massive stockpiles of supplies.[85] Oblivious to extraordinary demands about to be placed on the logistics system and confident of a quick victory, Halder ignored glaring vulnerabilities such as the expectations for supplies to be transported by trucks twice the distance regarded as feasible by logisticians.[86] Rarely in history has any campaign been based on such pervasive myths and empty hopes.

Ironically, in the crucial months between the fall of France and the invasion of the Soviet Union, German military leaders displayed few of the professional qualities that had led them to conduct a thorough assessment of the Polish campaign. Driven by a strong sense of urgency in the tense months before May 1940, they had rigorously identified and addressed the shortcomings in the September 1939 battles,[87] but they displayed little interest in such an assessment after May-June 1940.[88] Meanwhile, German commanders and staffs remained busy preparing an invasion of Britain, considering operations in Romania

and the Balkans, observing Italian actions in Africa, analyzing German interests in northwest Africa,[89] and designing "amphibian" tanks. In late October 1940, Halder studied a drive from Bulgaria across the Bosporus Straits to northern Syria to close the Mediterranean,[90] and as he worked himself into a "*Blitzkrieg* mania" he contemplated a huge operation across three continents against the strategic route between the Nile and the Euphrates.[91] Intoxicated by his success, Hitler thought in even grander but not necessarily clearer terms, dreaming of what Andreas Hillgruber has called a "world-wide *Blitzkrieg*."[92] German forces would push deep into Asia via Afghanistan to India and thereby threaten the British Empire.[93] Disconnected from reality, German strategy, which was more an *ad hoc* scheme than a formal *Blitzkrieg* strategy, remained hastily conceived and poorly designed.

Not until January and February 1941 did the approaching Russian campaign return the dreamers to solid ground and absorb the efforts of the entire *Wehrmacht*, but their attention was again diverted in April and May 1941 when German troops overran Yugoslavia, Greece, and Crete. Despite these distractions, most German leaders remained confident of success and agreed with Jodl when he said on January 18, "[T]he Russian colossus will be proved to be a pig's bladder; prick it and it will burst."[94] Few German leaders saw any need to doubt Hitler's comparison of a campaign against the Soviets to "a child's game in a sandbox."

Though blind arrogance and poor intelligence[95] explain much of the Germans' subsequent failure in the East, many of the disasters that befell their military forces stem from their distortions of the 1940 campaign and subsequent reliance upon those distortions in preparing for the 1941 invasion of the Soviet Union. In one of the greatest ironies of military history, the Germans fell victim to their own myth, or perhaps more correctly to their own disinformation campaign. They came to believe their press releases, movies, and propaganda, concluding that since they had

intended to use the *Blitzkrieg* against the French and had done so successfully, they could be just as successful against the Soviets. Recognition of the awesome difficulty of the task they had willingly accepted, however, came slowly to the German High Command. Halder recorded in his diary on July 3, the 12th day of the offensive,

> On the whole, then, it may be said even now that the objective to shatter the bulk of the Russian Army this side of the Dvina and Dniepr, has been accomplished. . . . It is thus probably no overstatement to say that the Russian Campaign has been won in the space of two weeks.[96]

The "make-believe spectacle," however, proved impossible to replicate against the Russians, and the Germans eventually fell victim to the myth of the *Blitzkrieg*. Despite Hitler's confidence and the German military's arrogance, the sand box proved to be an ice box, and the child's game the most demanding and self-destructive campaign in Germany's history.

ENDNOTES

1. See James R. Fitzsimonds and Jan M. Van Tol, "Revolutions in Military Affairs," *Joint Forces Quarterly*, Spring 1994, pp. 24, 28; David Jablonsky, *The Owl of Minerva Flies at Twilight: Doctrinal Change and Continuity and the Revolution in Military Affairs,* Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1994, pp. 16-17.

2. Williamson Murray, "Thinking about Revolutions in Military Affairs," *Joint Force Quarterly,* Summer 1997, p. 70.

3. Jeffrey R. Cooper, *Another View of the Revolution in Military Affairs,* Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1994, p. 14.

4. Steven Metz and James Kievit, *Strategy and the Revolution in Military Affairs: From Theory to Policy,* Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1995, pp. 14-15.

5. Michael Geyer, "Restorative Elites, German Society, and the Nazi Pursuit of War," in Richard Bessel, ed., *Fascist Italy and Nazi Germany:*

Comparisons and Contrasts, Cambridge: Cambridge University Press, 1996, p. 142.

6. S. J. Lewis, *Forgotten Legions: Germany Army Infantry Policy, 1918-1941,* New York: Praeger, 1985, p. 45. Larry Addington has described Guderian as the "dean of the German tank school" and credits him with creating the "general formula which characterized German armored warfare in the Second World War." Larry H. Addington, *The Blitzkrieg Era and the German General Staff, 1865-1941,* New Brunswick, NJ: Rutgers University Press, 1971, pp. 33, 34.

7. For recent German thought about the origins of the term, see Karl-Heinz Frieser, *Blitzkrieg-Legende: Der Westfeldzug 1940,* München: R. Oldenbourg, 1995, pp. 5-7.

8. "*Blitzkrieg*er," *Time*, Vol. XXXIV, No. 13*,* September 25, 1939, p. 25. Also see: Henry J. Reilly, "*Blitzkrieg*," *Foreign Affairs*, Vol. 18, No. 2*,* January 1940, pp. 254-265. For an example of those citing the use of the term in *Time*, see: Addington, *Blitzkrieg Era*, pp. 79, 234n. Sam Lewis argues that the word *Blitzkrieg* originated from Fritz Sternberg's *Germany and a Lightning War*, Edward Fitzgerald, trans.*,* London: Faber and Faber, 1939. Lewis, *Forgotten Legions*, p. 45n.

9. William J. Fanning, Jr., "The Origin of the Term '*Blitzkrieg*': Another View," *The Journal of Military History*, Vol. 61, No. 2*,* April 1997, pp. 284, 302.

10. In French writings, authors frequently used the term *attaque brusque* or *coup foudrant* to describe a swift blow aiming to injure an opponent seriously or to take him out of a war. They particularly appreciated the potential of such a blow given their high regard for Napoleon and his swift victories.

11. Fanning, "Origin of the Term '*Blitzkrieg*'," pp. 289-291. Karl Frieser observes that the word "*Blitzkrieg*" rarely appeared in official German publications even after the 1940 campaign. Frieser, *Blitzkrieg-Legende*, p. 6.

12. James S. Corum, *The Roots of Blitzkrieg: Hans von Seeckt and German Military Reform,* Lawrence: University Press of Kansas, 1992, pp. 37-43, 197-198.

13. Corum, *Roots of Blitzkrieg*, p. 203.

14. Corum, *Roots of Blitzkrieg*, pp. 137-141.

15. Lewis, *Forgotten Legions*, pp. 40-54.

16. Barry Posen, for example, describes Hitler as the "prime mover" in German innovation and describes his intervention as "decisive." Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars,* Ithaca, NY: Cornell University Press, 1984, pp. 74, 212, 218.

17. Erich von Manstein, *Lost Victories*, Anthony G. Powell, trans., Chicago, IL: H. Regnery, 1958, pp. 103-105.

18. Hans-Adolf Jacobsen, *Fall Gelb: Der Kampf um den Deutschen Operationsplan zur Westoffensive 1940,* Wiesbaden: Franz-Steiner, 1957, pp. 25-31.

19. Robert A. Doughty, *Breaking Point: Sedan and the Fall of France, 1940,* Hamden, CT: Archon Books, 1990, pp. 24-25.

20. Ulrich Liss, *Westfront 1939/40: Erinnerungen des Feindbearbeiters im O.K.H.,* Neckargemund: Kurt Vowinckel, 1959, pp. 106-107; Franz Halder, "Operational Basis for the First Phase of the French Campaign in 1940," Document MS # P-151, *World War II German Military Studies*, Vol. 12, pp. 10-13; Manstein, *Lost Victories*, p. 119; Heinz Guderian, *Panzer Leader*, Constantine Fitzgibbon, trans., New York: E. P. Dutton, Inc., 1952, pp. 90-91; Hans Umbreit, "The Battle for Hegemony in Western Europe," *Germany and the Second World War*, Vol. 2, "Germany's Initial Conquests in Europe," Oxford: Clarendon Press, 1991, pp. 246-247.

21. Walter Goerlitz, *History of The German General Staff, 1657-1945*, Brian Battershaw, trans., New York: Praeger, 1953, p. 368.

22. For a thorough assessment of the origins of the *Fall Gelb* plan, see Frieser, *Blitzkrieg-Legende*, pp. 71-116.

23. Frieser, *Blitzkrieg-Legende*, p. 435.

24. See Richard A. Preston, Alex Roland, and Sydney F. Wise, *Men in Arms: A History of Warfare and its Interrelationships with Western Society,* Fort Worth, TX: Holt, Rinehart and Winston, 1991, pp. 263-264; Hanson W. Baldwin, *The Crucial Years, 1939-1941,* New York: Harper & Row, 1976, pp. 124-126.

25. Doughty, *Breaking Point*, pp. 46-56; Frieser, *Blitzkrieg-Legende*, pp. 138-141; Florian K. Rothbrust, *Guderian's XIXth Panzer Corps and the Battle of France,* New York, NY: Praeger, 1990, pp. 53-55.

26. Doughty, *Breaking Point*, pp. 139-153; Frieser, *Blitzkrieg-Legende*, pp. 197-206; Rothbrust, *Guderian's XIXth Panzer Corps*, pp. 73-75.

27. Doughty, *Breaking Point*, pp. 162-164; Frieser, *Blitzkrieg-Legende*, pp. 211-213.

28. Doughty, *Breaking Point*, pp. 153-162; Frieser, *Blitzkrieg-Legende*, pp. 206-211; Rothbrust, *Guderian's XIXth Panzer Corps*, pp. 75-76.

29. Doughty, *Breaking Point*, pp. 202-213.

30. *Ibid*., pp. 235, 312-315.

31. J. F. C. Fuller, *A Military History of the Western World*, Vol. 3, New York, NY: Minerva Press, 1956, p. 382.

32. James S. Corum, *The Luftwaffe: Creating the Operational Air War, 1918-1940,* Lawrence, KS: University Press of Kansas, 1997, p. 275.

33. Doughty, *Breaking Point*, pp. 266-271; Frieser, *Blitzkrieg-Legende*, pp. 130-135.

34. Doughty, *Breaking Point*, pp. 134-137; Frieser, *Blitzkrieg-Legende*, pp. 188-189; Rothbrust, *Guderian's XIXth Panzer Corps*, pp. 71-73.

35. Doughty, *Breaking Point*, pp. 324, 3-4.

36. James S. Corum, "A Clash of Military Cultures: German and French Approaches to Technology between the World Wars," USAF Academy Symposium, September 1994, p. 7.

37. Doughty, *Breaking Point*, pp. 220-221.

38. Franz Halder, *The Halder Diaries: The Private War Journals of Colonel General Franz Halder,* Boulder, CO: Westview Press, 1976, Vol. 4, May 17, 1940, p. 17.

39. *Ibid*., May 18, 1940, p. 18.

40. *Ibid*., May 19, 1940, p. 19.

41. "Chancellor Hitler's Address to the German Reichstag," *Facts in Review*, Vol. 2, No. 32, August 5, 1940, p. 368.

42. Guderian, *Panzer Leader*, p. 106.

43. Corum, *Roots of Blitzkrieg*, p. 203.

44. Robert A. Doughty, *The Seeds of Disaster: The Development of French Army Doctrine, 1919-1939,* Hamden, CT: Archon Books, 1985, p. 189; Doughty, *Breaking Point*, p. 4.

45. Geyer, "Restorative Elites, German Society, and the Nazi Pursuit of War," p. 142.

46. For a survey of literature on the war in the east, see Rolf-Dieter Muller and Gerd R. Ueberschar, *Hitler's War in the East, 1941-1945: A Critical Assessment*, Bruce D. Little, trans., Oxford: Berghahn Books, 1997.

47. Quoted in Gerhard L. Weinberg, *Germany, Hitler, and World War II: Essays in Modern German and World History,* Cambridge: Cambridge University Press, p. 155; and Wilhelm Deist, *The Wehrmacht and German Rearmament,* Toronto: University of Toronto Press, 1981, p. 106.

48. At the Nuremberg Trials on February 8, 1946, General R. A. Rudenko, Chief Prosecutor for the Soviet Union, cited several instances of Hitler's conveying before the opening campaigns of World War II his intentions to obtain "living space" in Eastern Europe. See *Trial of the Major War Criminals before the International Military Tribunal, Nuremberg*, November 14, 1945—1 October 1946, Nuremberg, Germany, 1947, Vol. 7, p. 159.

49. Oberstleutnant Schmundt, *Bericht über Besprechung am* 23.5.1939, *Trial of the Major War Criminals*, Vol. 37, Document L-079, p. 548.

50. *Besprechung beim Fuhrer*, 23.11.39, *Trial of the Major War Criminals*, Vol. 26, Document PS-789, pp. 327-336; *Ansprache des Fuhrers vor den Oberbefehlshabern am* 22. Aug. 1939, *Trial of the Major War Criminals*, Vol. 26, Document PS-798, pp. 338-344.

51. *Besprechung beim Fuhrer*, 23.11.39, *Trial of the Major War Criminals*, Vol. 26, Document PS-789, pp. 330-331.

52. Walter Warlimont, *Inside Hitler's Headquarters, 1939-1945*, R. H. Barry, trans., New York, NY: Praeger, 1964, p. 114.

53. "Chancellor Hitler's Address to the German Reichstag," p. 361.

54. William L. Shirer, *Berlin Diary: The Journal of a Foreign Correspondent, 1934-1941,* New York, NY: Alfred A. Knopf, 1941, pp. 455-456.

55. Walter Gorlitz, ed., *The Memoirs of Field-Marshal Keitel*, David Irving, trans., New York, NY: Stein and Day, 1965, p. 118.

56. Shirer, *Berlin Diary*, p. 452.

57. *Ibid*., p. 453.

58. *Halder Diaries*, Vol. 4, July 13, 1940, p. 117.

59. *Ibid*., July 22, 1940, p. 126.

60. *Ibid*., pp. 126-128.

61. *Ibid*., p. 128.

62. *Ibid*., July 3, 1940, pp. 101, IV-5.

63. *Ibid*., July 27, 1940, p. 134.

64. *Ibid*.

65. *Ibid*., July 28, 1940, p. 135.

66. *Trial of the Major War Criminals*, Vol. 15, Testimony of General Alfred Jodl, June 5, 1946, p. 390.

67. Warlimont, *Inside Hitler's Headquarters*, p. 111.

68. *Halder Diaries*, Vol. 4, July 31, 1940, pp. 144-145.

69. Albert Speer, *Inside the Third Reich*, Richard and Clara Winston, trans., New York, NY: Collier Books, 1981, p. 173. Cited in Barry A. Leach, *German Strategy against Russia, 1939-1941,* Oxford: Clarendon Press, 1973, p. 55n.

70. See, for example, Halder's comment on September 14 about Operation SEA LION not being called off. *Halder Diaries*, Vol. 4, September 14, 1940, p. 194.

71. Leach, *German Strategy against Russia*, pp. 60, 101-103; Bryan I. Fugate, *Operation BARBAROSSA: Strategy and Tactics on the Eastern Front, 1941,* Novato, CA: Presidio Press, 1984, pp. 63-69.

72. Fugate, *Operation BARBAROSSA*, pp. 69-71; Leach, *German Strategy against Russia*, pp. 108-110.

73. Fugate, *Operation BARBAROSSA*, pp. 72-73; Leach, *German Strategy against Russia*, pp. 103-106.

74. An extract of Marcks' study is included in Leach, *German Strategy against Russia,* p. 253.

75. An extract of Lossberg's study is included in Leach, *German Strategy against Russia*, p. 255.

76. *The Fuhrer and Supreme Commander of the Armed Forces, Directive No. 21*, Operation "Barbarossa," Fuhrer Headquarters, December 18, 1940, German Military Documents Section, Fuhrer Directives and Other Top-Level Directives of the German Armed Forces, 1939-1941*,* Washington, DC: typescript, 1948, pp. 127-128.

77. Frieser, *Blitzkrieg-Legende*, p. 438.

78. Klaus Reinhardt, *Moscow—the Turning Point: The Failure of Hitler's Strategy in the Winter of 1941-42*, Karl B. Keenan*,* trans., Oxford: Berg, 1992, p. 11.

79. *Halder Diaries*, Vol. 4, July 22, 1940, p. 128.

80. Reinhardt, *Moscow—the Turning Point*, p. 11.

81. Alan S. Milward, *The German Economy at War,* London: Athlone Press, 1965, p. 11.

82. Williamson Murray, "Force Strategy, *Blitzkrieg* Strategy and the Economic Difficulties: Nazi Grand Strategy in the 1930s," *Journal of the Royal United Service Institute for Defence Studies*, Vol. 128, No. 1*,* March 1983, pp. 39-43.

83. Frieser, *Blitzkrieg-Legende*, pp. 30-31.

84. Andreas Hillgruber, *Germany and the Two World Wars*, William C. Kirby*,* trans., Cambridge, MA: Harvard University Press, 1981, p. 79.

85. R. H. S. Stolfi argues that the German logistical system was appropriate for a short campaign and that German failure came not from inadequate supplies but from Hitler's misdirecting the campaign in late summer and thereby throwing away an almost-certain victory. R. H. S. Stolfi, *Hitler's Panzers East: World War II Reinterpreted,* Norman, OK: University of Oklahoma Press, 1991, pp. 166-167.

86. Leach, *German Strategy against Russia*, p. 139.

87. Williamson Murray, "The German Response to Victory in Poland: A Case Study in Professionalism," *Armed Forces and Society*, Vol. 7, No. 2, Winter 1981, pp. 285-98.

88. Hillgruber, *Germany and the Two World Wars*, p. 80.

89. Norman J. W. Goda, *Tomorrow the World: Hitler, Northwest Africa, and the Path toward America,* College Station, TX: Texas A&M University Press, 1998, pp. xiv-xxvi; Charles B. Burdick, *Germany's Military Strategy and Spain in World War II,* Syracuse, NY: Syracuse University Press, 1968.

90. *Halder Diaries*, Vol. 4, October 28, 1940, p. 251.

91. Frieser, *Blitzkrieg-Legende*, pp. 438-439.

92. Andreas Hillgruber, *Hitler's Strategie: Politik und Kriegfuhrung 1940-1941,* Frankfurt am Main: Bernard & Graefe, 1965, p. 317*ff*. Hillgruber, *Germany and the Two World Wars*, pp. 88-89.

93. Frieser, *Blitzkrieg-Legende*, p. 439.

94. Warlimont, *Inside Hitler's Headquarters*, p. 140.

95. For a different assessment, see Stolfi, *Hitler's Panzers East*, pp. 18-20.

96. *Halder Diaries*, Vol. 6, July 3, 1941, p. 196.

ASYMMETRIC RESPONSE TO AMERICAN AIR SUPREMACY IN VIETNAM

Donald J. Mrozek

INTRODUCTION

In the 1960s and 1970s, the United States enjoyed an abundance of power and a broad range of military capabilities. During the Vietnam War, the U.S. government sought to use that power asymmetrically, sometimes substituting technology for manpower, at other times using its military capabilities to alter the conditions of the war and the means for its prosecution. Yet it was unable to achieve a military victory—even a military stalemate—despite a spectacular application of military force in the longest war that the United States ever fought. Enjoying overwhelming superiority in air power against Viet Cong and North Vietnamese forces, the United States ultimately proved unable to convert its power into enemy compliance with its policy.

A key source of frustration throughout the war was the sense that the enemy was not playing fair, refusing to follow rules taken for granted among technologically and organizationally superior states. Guerrilla tactics, assassination, terrorism—these were methods that Americans found difficulty in describing as truly "war" at all. At the same time, to the extent that the North Vietnamese Army (NVA) seemed to be the more important enemy force, counterinsurgency seemed a distracting waste of human and material resources. How could the United States make its enemy—or, operationally, its enemies—respond on American terms to asymmetrical applications of military power? How could the United States be "*in* the war but not *of* it," forcing the enemy to accede to American will without adopting the enemy's way of war?

In addressing this challenge, we expected air power to play many important roles—but roles reflecting competing strategic visions. U.S. officials were quick to agree that air power should be used in Vietnam to take advantage of an American strength, but they did not agree on precisely what "air power" meant or on a theory and strategy for its employment. Could "air power" address the spectrum of conflict from guerrilla through conventional action in the difficult environment of Vietnam? Or was this just the piecemeal application of specific "air assets" in ways that diminished true air power? Could asymmetrical use of air power substitute for unattractive options such as protracted operations and occupation on the ground? Could asymmetrical use of air power achieve the goals of policy, or could it merely achieve specific tasks that, taken together, offered no guarantee of a larger result? In the end, the Vietnam War gave Americans dramatic and painful evidence of the limitations of military power and of the fact that, in the end, military power is not abstract or generic.[1]

ASYMMETRY IN THE AMERICAN MILITARY EXPERIENCE

Asymmetry in the conception and conduct of American military affairs dates back at least to the arrival of European settlers. At Jamestown (1607), transplanted Englishmen offset their tiny numbers by firing cannon to "overawe" the local Indians, seeking to turn technological asymmetry into long-term strategic advantage in a pre-emptive act of deterrence. In King Philip's War (1675-1676), New England colonists revised their way of war in the midst of the conflict, adopting tactics largely symmetrical with those of their Indian enemies while newly espousing systemic attrition and annihilation instead of mere victory in discrete battles. The Seven Years' War (1754-1763), also called the French and Indian War, saw both symmetry and asymmetry—with Edward Braddock, his British regulars, and American auxiliaries decimated at the Battle of the Wilderness by a French and Indian force

differently composed and uncommitted to the current customs of warfare in Europe, while on the Plains of Abraham, late in the war, James Wolfe's forces battled those of Louis Joseph, Marquis de Montcalm, with both combatants operating on essentially the same military assumptions and conventions. Indeed, colonial American military experience may be viewed as a dialogue between those settlers who sought to create an armed force as much like those of the European powers as possible and other settlers who came to see irregular forces as having unique virtues explicitly suited to American circumstances.

This tension continued to characterize American military affairs after 1789. Throughout the 19th century, civilian and military leaders of the U.S. armed forces sought to build military institutions based on European models that were deemed scientific, intrinsically superior, and "state of the art" while, often at the same time, conducting wars in which adversaries did not share the same ideas about the "conventions of war." In the First Seminole War (1816-1818), Andrew Jackson led a campaign into Spanish Florida, pursuing a generally conventional strategy of seizing Spanish strong points by generally conventional means. The causes of the war had to do with African Americans and Native Americans who were engaged in irregular fighting, but the larger structure of the conflict and the military means used for its resolution conformed to conventional European models. This was possible because, in the end, it was a conflict between the United States and Spain rather than a conflict between U.S. regulars and indigenous insurgents. But in the Second Seminole War (1835-1842), the U.S. Army faced an elusive enemy that did not share the commitment to Napoleonic strategy and tactics displayed by U.S. generals such as Winfield Scott. As Russell Weigley put it, while "attempting to trap the main body of hostiles in their lair . . . , [Scott's] heavy columns of slow-moving troops and much impedimenta marching noisily through the Florida hammocks merely served to scatter the Seminoles, so that Scott's blows landed in the

air."[2] All the more pertinent for its resonance with events 130 years later was the asymmetry of situation, vision, and valuation of consequences that Weigley summarized this way:

> The standard strategic objectives of European war, strategically located fortresses, lines of communication, and political centers, could not be pursued because they did not exist. For seven years, from 1835 to 1842, one general after another damaged his military reputation in Florida in the frustrating pursuit of enemies who seemed solid only when they were striking out in ambush, but who apparently changed into ghosts as soon as they were struck in turn.[3]

In the end, the announced object of the war—removing all Seminoles from Florida—was not achieved, and what *was* eventually achieved came by means that Weigley has described as "treachery and brutality," including, for one, the repudiation of a truce by Brevet Major General Thomas S. Jesup to take advantage of the ill-gotten opportunity to capture Seminole Chief Osceola and, for another, the pursuit of a scorched earth policy of burning Indian villages and crops. In the end, what allowed U.S. forces to exact some substitute for the desired victory was neither asymmetrically superior numbers, asymmetrically advanced technology, nor asymmetrically elevated strategy, but rather a radical—and highly controversial—resort to methods widely deemed inhumane, inappropriate to a civilized society, and opposed to core values of American military professionalism.

Later in the century, American wars often hinged on asymmetrical advantages that were exploited within largely symmetrical visions of warfare shared by both sides to each conflict. In its War with Mexico (1846-1848), the United States benefitted from an asymmetrical edge in organizational skills.[5] In the American Civil War (1861-1865), Union success ultimately depended not on "decisive victory" in battle between two similarly organized, similarly manned, and similarly armed forces but on the adoption of an asymmetrical strategic vision, originally

foreseen by Winfield Scott and eventually executed by Ulysses Grant and William Sherman, which looked beyond specific battles to the decisiveness of a grand campaign mobilizing long-term economic superiority and other distinctive advantages. In the Spanish-American War (1898), too, U.S. victory depended on such asymmetrical advantages as more modern warships and superior training and élan.

But matters were fundamentally different wherever the United States faced adversaries who did not share current conventional thinking as to the character and customs suitable to warfare in the modern age. Much of the history of the U.S. Army's fight with the Indians of the Great Plains and the West exemplifies this phenomenon.[6] The extension of military and political dominance over independent-minded Native American tribes depended not only on the superior resource base and technology of the European Americans. It hinged also on applying to the trans-Mississippi West the Civil War conceptual breakthrough that Weigley has called a "strategy of annihilation."[7] This change facilitated the adoption of an offensive strategy, enabling the U.S. Army to operate with greater localized weight and effectiveness. So, then, a mutation in grand strategic thought in Washington triggered a change in how the Army operated, with the result that its asymmetrical technology, training, and other advantages could be exploited.[8] Even so, full security in what had been the frontier sometimes came at the price of approximating the Indians' own tactics and manner of warfare, as George Crook did against the Apaches in the 1880s.[9] In such cases, success required *reducing* the asymmetry between the opposing forces and in their manner of operation.

Another case in point was the fight against the Filipino "insurrectos" led by Emilio Aguinaldo, whom the United States had brought back from exile in 1898 specifically for the purpose of conducting an insurgency to subvert Spanish control of the islands. In the end, only the sanctioning of techniques that Americans had first dismissed as

unprofessional and dirty—with guerrilla and counter-guerrilla action that became scandalous enough to trigger a major Congressional investigation—allowed a favorable compromise that promised, but delayed, Philippine independence.[10] Still less successful was the U.S. effort against the Moros on Mindanao, where resistance to American rule remained vigorous long after it had been accepted on Luzon. Here U.S. forces fought a frustrating counterinsurgency for another dozen years, without having achieved the subjugation of the Moros. Asymmetrical advantages in weapons helped to limit U.S. casualties and to protract the American presence but did not suffice to achieve the real objective. In the end, the Americans settled for a redeployment that was not officially recognized as failure.

The American military experience is rich in cases where asymmetry in technology, resources, strategic vision, and other critically important elements have been determinative, whether accounting for victory or defeat. At the same time, Americans have been slow to treat asymmetrical conflict as an inevitable fact in the life of the United States as it moved through expansionism to global power, instead dismissing it as anomaly and error. The U.S. achievement and retention of great power status in the 20th century has obscured the fact that specific military failures—indeed, defeats—punctuate the national military record and that ill-appreciated asymmetries go far toward explaining them.

THE ROOTS OF U.S. MILITARY "UNIVERSALISM"

The belief that, at any given time, there is one right way to organize an armed force and, basically, one right way to use it has had persistent appeal throughout most of U.S. history. On the other hand, Americans have sometimes found themselves forced to yield to exigent circumstances, departing from the way deemed right. The desire for the explanatory simplicity of a "one size fits all" military policy

has stumbled over the distinctive conditions and different mentalities encountered in specific conflicts.

Cultural, intellectual, and political history suggests how this problem emerged and why it has endured. In essence, the fundamental political institutions of the United States have been shaped by the ideas and instincts of the Enlightenment. Central to Enlightenment thought is a profound universalist bias. The statement that "*all* men are created equal" is just one rhetorical example of the belief that human nature dictates one ideal form of government, which in turn suggests one ideal way of making war and securing peace. The Enlightenment spirit, then, is all about the application of one set of rules and one set of expectations to all peoples and all situations. At first, Americans experimented with new organizational models and new strategic ideas that presumably derived from the revolutionary implications of democratic politics. The democratic decentralism of the coastal gunboat system of Thomas Jefferson and the plan for a militia navy are failed manifestations of that idea. Eventually, commitment to a militia system yielded to the idea of military professionalism, but the concept of professional expertise preserved the illusion that universal principles and criteria applied to all institutions. The earlier notion of universal political truths was now linked with that of universal technical imperatives. In short, the ever more scientific character of war supposedly canceled out local preferences and distinctiveness.

A second force—Social Darwinism—imposed a "dog-eat-dog" competitive dynamic that ultimately exalted a hierarchy among nations ultimately based on power, certainly including social and economic power but finally ensured by physical force. Victory went to the biggest dog with the sharpest bite, and some breeds were seen as distinctly better than others. The universalism of the Enlightenment survived in Social Darwinism, but shorn of its egalitarian aspirations, and, in place of that, specialized expertise—and professionalism—became the mark of

excellence. Bigger was better than smaller, intricacy was superior to austerity, order was preferable to intuition, and ardent devotion to authority displaced passionate commitment to one's own beliefs. This kind of thinking carried two prospectively fatal flaws. First, it tended to obscure the highly specific nature of military power—the fact that it is not "generic." Second, it masked the great capacity for resistance enjoyed by a people inferior in technology and in many other areas, provided that they rejected the underlying social theory on which Western imperial dominance depended.

The modern era, characterized by industrialization, a global system of nation states, and the predominance of the Western organizational ethos, has been built on the assumption that a world order can be created on the basis of universal principles. It has also been coincident with "universalist" military thinking.[11] More specifically, military theories of air power and nuclear warfare after World War II fostered a taste for escalation so as to deny the enemy the choice of weapons, a belief that disproportionately great application of force would overwhelm any enemy, and the conviction that something bad in the present could be stopped by threatening something worse in the future. Although the nuclear competition between the United States and the USSR was following a largely symmetrical track, this did nothing to undercut the expectation that asymmetrical use of military power, using much the same forces in substantially the same ways in just about any conditions, would deter an enemy and, if applied too late for deterrence, would make the enemy desist. But Vietnam-era Americans had difficulty believing that the "weaker" the enemy as judged by conventional standards, the harder the challenge of defeating it.

EXAMPLES OF 20th-CENTURY INSURGENT THOUGHT

During the 20th century, nationalist leaders in countries under foreign imperial control or in colonial status

developed theories of resistance that recognized the inferiority of their armed forces and sought ways of maximizing the impact of whatever powers they did possess. All these theories ultimately saw time as the great advantage disproportionately enjoyed by the conventionally weaker force, largely because of the great costs, both material and moral, entailed in sustaining a modern military presence and in seeking to pacify entire populations. It was not that democracies could not fight long wars—rather, it was modern industrialized warfare itself that was seen as carrying the potential for its own frustration. The longer the war and the wider the distribution of forces in pursuit of an elusive enemy, the weaker the modern industrialized force would become and the more vulnerable it would be to such force as its enemy possessed.[12]

Perhaps the strongest statement of this case was made by Mao Zedong. Although written from a Chinese perspective and overtly focused on East Asian conditions, the military works of Mao created a scenario of "empowerment" that depended primarily on exploiting asymmetry in operational assumptions and tactics so that a seeming weakness would become an unbeatable strength. Commitment to resist indefinitely coupled with the idea of "trading space for time" was to exhaust the Japanese by spreading them too thin, by exposing lines of supply and communications, by creating opportunities for counterattack first at the guerrilla level but eventually by conventional means, and by demoralizing the enemy at home. Mao developed this formula for resistance in response to the Japanese invasion of eastern China in 1937, but it was still at work a quarter century later in Vietnam.[13]

At the same time, insurgent forces recognized that a conventionally superior opposing force could be made to act in ways that entailed great political costs for the government it served. In the pacifist vision of Gandhi, for example, non-violent civil disobedience might be met by violent action on the part of the conventionally armed force,

but this would cause a transforming revulsion among the conventionals at the violence they were inflicting on a peaceful, though non-compliant, population. In *The Wretched of the Earth* (1965), Frantz Fanon took a less promising view of human nature but still saw the escalation of violence by one's enemy as advantageous.[14] The more violently a government could be made to act against an insurgent element, the more the government's legitimacy would be compromised.[15]

Theories such as these clearly put priority on political conditions over military ones. The lens of politics determines how military action is understood. In this sense, military action itself does not produce political change, although it may produce conditions and opportunities in which political change can be enforced. Earlier American experience, as already noted, had given evidence of this relationship and had revealed both the strengths and the limits of an asymmetrical dynamic. For example, there was a great difference between the dynamic of the so-called *insurrectos* of the Philippines and that of the Moros, the former of which were ultimately brought to accede to long-term U.S. authority over the Philippines and the latter of whom never really were. To the extent that U.S. forces were effective, especially with the Moros, it was because they adapted substantially to the "way of war" of their enemy. Exclusive reliance of the Americans on the asymmetrically superior organization, weaponry, and other assets could not have yielded such broad objectives as enduring pacification. Even with Aguinaldo and his followers, moreover, it was a framework of U.S. political concession to the Filipinos that allowed for a cessation of hostilities.

Theories of insurgent resistance, in which local conditions predominate and in which one's own seeming weaknesses are to be converted into strengths, conflicted sharply with the modernist ideas of air power theorists whose vision of future wars was focused on large scale and high technology.[16] Concepts such as pinpoint strategic

bombing of vital elements of an enemy's industrial infrastructure made sense in an environment where symmetry of strategic aspiration prevailed even in the face of asymmetry in resources and their development. But could such action change the will of the enemy—especially the will of a technologically less sophisticated country? What if the enemy had already psychologically written off the assets threatened by air attack? Was it the *threat* of air attack that was expected to produce the political change, or was it that direct material *effects* of air attacks were expected to so greatly change material conditions as to force a different political result regardless of the enemy's intentions?

One of the great ironies in the American effort to use air power to oppose insurgency in Vietnam is the extent to which it corresponded to guerrilla theorists' predictions of what would occur. As with Mao, so with Ho Chi Minh and Vo Ngyuen Giap, the presumptive unpopularity of the purposes of the adversary—whether Japan, France, or the United States—would leave it with only material advantages to exploit. Strategic, political, and moral force rooted in local conditions would remain the strength of the resistance.[18] Even allowing for the quasi-religious appeal to asceticism and service that characterizes Che Guevara's writings, for example, the faith in the political commitment of local groups was not mere romanticism. The fundamental presupposition was the universal validity of dialectical materialism playing itself out through time in undeniable "objective conditions"—a distinctly modernist and universalist vision. In this sense, it is precisely the modernist, universalist pretension of communism that ensured its unsuitability to a host of contexts upon which it was imposed and, in retrospect, that now seems to have ensured its ultimate failure on the world scene, even though it served nationalist purposes in several local settings. At the same time, however, the modernist, universalist impulse in the American experience fostered a belief in the generic quality of military force—for example, that more is apt to be better and that successive advances in weapons

would allow those employing them to address not only the greatest military challenges but the great array of lesser military problems as well. In essence, a sufficient qualitative advance as embodied in an advanced weapon system would obviate qualitative differentiation of military problems at lesser levels.

CONCEPTUAL ASYMMETRIES AND VIETNAM

In retrospect, the most radical asymmetries of all in the decades after World War II were those related to "subjective conditions" rather than "objective" ones. The myth of modernist "scientific" uniformity in the Soviet Union itself and in the communist bloc in Eastern Europe was shown false as soon as the authoritarian elite lost its grip. Nationalist passions of a most unscientific sort—left unattended for decades and, in some instances, for generations—not only accelerated the collapse of the old Soviet system but, after its collapse, continued to complicate security planning in such places as the former Yugoslavia. But these same nationalist passions had driven developments in Southeast Asia after World War II. The great difference, easier to see several decades after the fact, was the comparative autonomy of communist nationalisms in Asia, especially when judged against the authoritarian oppression of Stalinism in Eastern Europe.[18]

A second conceptual asymmetry pertained to the meaning given to escalation and de-escalation—or, more generally, to tempo and intensity. Intentionally or not, most U.S. leaders came to see the movement to higher levels of escalation as enhancing the possibility of decisive outcome, as if a higher level of warfare, once reached, could not be abandoned by a combatant without fatal damage to the capacity to resist. Only a few Americans theorized—as Walt Rostow did as early as 1961—that the fighting in Southeast Asia might never be formally called off but merely subside to comparative insignificance.[20] By contrast, typical of U.S. leaders, General Westmoreland saw the movement from

guerrilla action to mobile warfare in 1964 as "the beginning of the final phase of the war."[21] This conventional thinking conflicted completely with what Mao, Giap, and others had always allowed—namely, that the manner and intensity of warfare did not need to go steadily upward for the insurgency to succeed. A downturn in intensity, or a return to guerrilla action after a period of mobile warfare, could also be a legitimate step toward final victory. As long as the political base—the "sea of the people" in which Mao's guerrilla "fish" swam—remained secure, the war could go on without end. This conceptual asymmetry goes far to explain why U.S. officials could have hoped for so much from air power and why, in the end, it could have produced so much less than had been expected.

The dynamics in the use of air power in Vietnam also owed much to prevailing views of what strategic armaments had accomplished in the global confrontation between the United States and the Soviet Union. Presumably, the credible threat to use U.S. strategic nuclear forces in massive retaliation had deterred the Soviet Union from expansionist adventurism. A well calibrated threat had presumably changed their minds. If so, then why couldn't the threat of retaliation—not nuclear but disproportionately great compared to the actions of the enemy—change the minds of North Vietnamese leaders? Part of the problem was that the Vietnam War was, in a sense, not one war but several successive and overlapping wars—internally inconsistent and asymmetrical, the balance of its elements changing over time. In the early 1960s, for example, both civilian and military leaders in the United States widely recognized the insurgency in southern Vietnam as indigenous, even if they were also keenly aware of Hanoi's supporting and coordinating role.[22] In this more complicated version of the war, calculating the political results of military action was essentially a matter of perspective. Specific symmetrical battles in which the Viet Cong and NVA were technically defeated still contributed to strategic victory because, even when battles themselves

were fought in a largely symmetrical manner, they served asymmetrical strategies so that a string of "defeats" really constituted a victory in the making.[23]

In reality, the imposition of a nuclear bipolar model onto regional conflict was inappropriate to the situation. In the global confrontation, the opposing forces were symmetrically structured, broadly speaking, and strategic operational expectations were largely the same. But in Southeast Asia, this was not the case. Forces were asymmetrically composed and, more important, guided by asymmetrical strategic rationales. Holding Soviet assets as "hostage" to Soviet good behavior was echoed in holding valuable North Vietnamese targets in reserve as "hostage" to anticipated changes in Hanoi's war policy. But this ignored the fundamental differences in strategy between Moscow and Hanoi as well as between Hanoi and Washington.

Another line of thought concerning Vietnam is that much of its baseline asymmetry was illusory and, bluntly put, that it would have been better to treat the Vietnam War more like the Korean War. In his influential study *On Strategy: The Vietnam War in Context* (1981)[24], Colonel Harry G. Summers, Jr., criticized U.S. leaders of the Vietnam era, alleging that they had directed too much attention to counterinsurgency and had credited insurgents in the south with too much autonomy. Viet Cong action was a sideshow or even a deception, with U.S. leaders taken in by it. Yet many key figures, such as Walt Rostow, emphasized the link between Hanoi and the Viet Cong from the start. What changed was not the perception of ties between the Viet Cong and Hanoi but the results expected from the use of American air power and other assets. They were first intended as a statement of U.S. determination and as a "message" that Hanoi should change its policy, and then increasingly were meant to interdict the flow of supplies regardless of enemy intentions. Viewed from another vantage, what precluded an approach in Vietnam more like the one taken in Korea was the weakness of the

Saigon regime.[25] Arguably, there was much success in developing the Army of the Republic of Vietnam (ARVN)—but much less in forging an effective and unifying political force in the south. In fact, it is arguable that the piecemeal U.S. escalation in the early- through mid-1960s conformed more to political deterioration in the south than to military adventurism in the north. If the United States was not its own worst enemy in this matter, perhaps its ally was.

ASYMMETRICAL USES OF AIR POWER[26]

Among the most salient characteristics of the Vietnam War was that the United States enjoyed air control over South Vietnam and air superiority throughout Southeast Asia during the entirety of the conflict. One can only imagine the excuses for the failure of the American venture that might have been offered if air operations, especially over the South, had been seriously contested and impeded. One essential fact, then, is that the United States pursued this war while enjoying what has been perceived as a huge asymmetrical advantage—air superiority and, in some times and places, even clear air control.[27] Enemy anti-aircraft artillery and surface-to-air missiles were serious problems, to be sure, but the pre-eminence of U.S. air power in the region created a special context that encouraged its asymmetrical use. Let us discuss four of these asymmetrical uses: aerial firepower, site defense (gravitating to interdiction), interdiction (gravitating to "sending messages"), and air mobility.

Aerial Firepower.

The asymmetrical advantage in air power possessed by U.S. forces allowed President Johnson and General Westmoreland to rely on aerial firepower in defense of the U.S. Marine base at Khe Sanh in 1968. Indeed, without air power, the decision to establish the base, let alone to defend it, would have been militarily questionable and politically

implausible. Nor was defense of this specific location the main point. Westmoreland's purpose at Khe Sanh was to draw the interest of the enemy and to do what he had wanted to do all along—in Bernard C. Nalty's words, "to engage the enemy so that America's awesome firepower (everything from M-16 rifles to B-52 bombers) could be brought to bear. His objective was not to capture a hill or ridge line, but to destroy enemy soldiers and hostile units." Like the French at Dien Bien Phu in 1954, the Americans at Khe Sanh in 1968 were luring the enemy with the hope of a dramatic victory, thereby trying to bring them to battle on terms that would best exploit the technological and other advantages held by U.S. forces. Unlike the French, who had just 200 planes per day on which to rely in the best of circumstances, the Americans "could draw upon a Southeast Asian armada of 2,000 planes and 3,300 helicopters."[29]

According to General Westmoreland, the purpose of massed aerial firepower was to guarantee "our ability to preempt or blunt . . . a concerted attack."[30] In 1967, when the enemy was besieging Con Thien, tactical aircraft and B-52s had been brought to bear in close coordination with naval gunfire and artillery. The great volume of fire and its withering effect on the enemy convinced Westmoreland that "massed firepower was *in itself sufficient* to force a besieging enemy to desist, a demonstration that was destined to contribute to my confidence on a later occasion" (Westmoreland's emphasis).[31] Westmoreland expected the encounter at Khe Sanh to claim large numbers of North Vietnamese and Viet Cong and to cost few U.S. and South Vietnamese men. He later claimed that loss were 8 to 1 in favor of the United States and South Vietnam.[32] Senator J. Strom Thurmond expressed the view that 75 percent of the Viet Cong killed in the war had fallen to artillery fire and air assaults, including bombs dropped from B-52s. To Thurmond as to Westmoreland, aerial firepower contributed to the safety of U.S. fighting men on the ground.[33] Between mid-January and late March 1968, the

contribution at Khe Sanh included some 10,000 Air Force fighter strikes, more than 5,000 Navy and 7,000 Marine strikes, and more than 2,500 B-52 strikes—upwards of 24,500 in all. Cells of three B-52s left their bases on Guam and in Thailand every three hours, putting B-52s over Khe Sanh every hour and a half. Arc Light, Mini-Arc Light, and Micro-Arc Light strikes were designed to meet different target demands and time constraints, with Mini-Arc Lights taking roughly 45 minutes to plan and execute and Micro-Arc Lights merely 10 minutes. Finally, the siege was broken, and the enemy disengaged. U.S. officers claimed a great success, General Westmoreland calling the whole enterprise "an awesome display of firepower . . . one of the heaviest and most concentrated in the history of warfare."[34] Historians Peter B. Mersky and Norman Polmar suggest that the B-52 Arc Light strikes were ultimately the single most critical element in the firepower delivered, concluding that they "finally evidently broke the enemy's resistance."[35]

But just what was the accomplishment? To be sure, air crews had performed brilliantly, and, even allowing for overlapping air control systems and other problems, there was cause for pride in the support given to the men at Khe Sanh. Indeed, the resistance was "broken" if resistance meant the coordinated siege of Khe Sanh itself. But the enemy was by no means finished. In discussing Khe Sanh and other aspects of the Vietnam War, military officers often described the same event as both offensive and defensive. For example, they talked of the "defense" of Khe Sanh, the "siege" of Khe Sanh, and the "relief" of Khe Sanh. Such terms suggested that the North Vietnamese had the initiative. But Westmoreland wanted to call it an "offensive in place," asserting that the United States was winning a genuine victory by grinding down enemy forces with firepower. The common understanding of an "offensive" as incorporating positive geographical movement was being challenged by the belief that air assets could conduct an "offensive" in one place. It is important to note that this interpretation of Khe Sanh and air power's role in its

defense permitted General Westmoreland to maintain his understanding of the Vietnam War substantially intact.[37] Whether this result was a positive one is open to dispute.

General Westmoreland's optimism might well have been tempered by events at the special forces camp at Kham Duc in April and May 1968, where North Vietnamese and Viet Cong were active building roads and other infrastructure of precisely the sort that an American presence in the region was intended to prevent. One after another, Kham Duc's seven outlying posts were attacked, falling to enemy assault despite the use of U.S. aerial firepower. B-52 attacks failed to stop the enemy, and resupply of Kham Duc quickly became problematic. The evacuation of Kham Duc prevented a massacre, preserving the cherished notion that the Americans never lost a battle to the North Vietnamese and the Viet Cong. But it also made quite clear that air power was no cure-all. The Tet Offensive was put down, Khe Sanh was relieved, and Kham Duc was evacuated—but where was the plan for victory? Where was the U.S. offensive? Was the offensive "in place" anywhere but in the hopes and the imagination of U.S. leaders?

From Site Defense to Interdiction.

The case of fixed-wing gunships provides an example of innovative application of asymmetrical force in tactical situations that improved the chances for successful operation on the ground, but it also illustrates how application of this same asymmetrical element for quite different purposes could produce ambiguous or even negative results.[38] The idea of using relatively slow fixed-wing aircraft with side-mounted guns to provide aerial fire support for support of ground forces was proposed to the Tactical Air Command (TAC) in 1961. Basically, it originated among individuals concerned with counterinsurgency, then moving through experimentation and testing as through a thicket of bureaucratic indifference and suspicion in a process historian Jack S. Ballard has

called "crablike." Against opposition views that the C-47 gunship (later AC-47) was too vulnerable, TAC was charged with using the gunships in combat, notably in support of the counterinsurgency effort.[39]

The special effectiveness of the gunships in night operations made them popular with the units they supported. According to Air Force Captain Ronald W. Terry, a strong advocate of fixed-wing gunships, operations to defend forts and hamlets at night were so successful that this became "the only thing we ever got to do."[40] On December 23, 1964, for example, a gunship on airborne alert was sent toward Thanh Yend, which was under heavy Viet Cong attack, while another was sent to aid Trung Hung. In the latter case, defenders attested that the Viet Cong broke off the attack as soon as the gunship opened fire. Hope rose that areas designated as safe by the Saigon government might actually become so. Operations at Ngai Giao on December 28, 1964, and in the Bong Son area on February 8, 1965, gave further evidence that gunships might be changing the balance on the ground. At Bong Son, some 20,500 rounds were fired and about 300 Viet Cong were killed. Now convinced of the value of the gunships, the Air Force determined to send a squadron of gunships to Vietnam on a permanent basis with deployment to be completed by November. Seventh Air Force's Operations Order 411-65 specified the mission: "to respond with flares and firepower in support of hamlets under night attack, supplement strike aircraft in defense of friendly forces, and provide long endurance escort for convoys."

Despite this early success with gunships in support of ground combat, however, attention soon shifted to using them to interdict Viet Cong supply, particularly if the gunships' night capabilities could be enhanced. It was estimated that 80 percent of Viet Cong supplies were moved at night. But the changes made to the gunships with this important problem in mind turned the gunship program from site and convoy defense, where it seemed to be working, to interdiction, where it was unproven. Air Force

officers who had opposed the gunship program because of the operational limitations of the AC-47 now sought to enhance or replace it, either with the AC-119 favored by Secretary of the Air Force Harold Brown or with the AC-130 advocated by the Air Staff. The Air Staff wanted AC-130s deployed in Southeast Asia for around-the-clock interdiction of enemy supply routes through Laos. Secretary Brown regarded the AC-119 as useful for "more localized support and [a] protective role" and the AC-130 as serving "the predominantly search-and-destroy concept."[41] Nonetheless, by 1969-1970, evaluators from U.S. Air Force, Pacific rated the AC-119 as effective because "it was capable of destroying trucks and attacking targets as assigned," while noting that the AC-130 had always had as its primary mission "night interdiction and armed reconnaissance to destroy wheeled and tracked vehicular traffic on roads and sampans on waterways."[42]

The movement toward interdiction became an irrepressible theme in gunship operations. Ironically, however, the impact of gunships diverted from interdiction to their original purpose was clear at the end of the 1960s, even as doubts about the overall effectiveness of gunships in the interdiction effort rose sharply. On August 23, 1968, for example, a Civilian Irregular Defense (CIDG) and Military Assistance Command Vietnam (MACV) compound at Duc Lap in Quang Duc province was convincingly supported.[43] The withdrawal from Ngoc Tavak, a forward outpost of the Kham Duc base, depended on AC-47 Spooky gunships, recalling their earlier principal purpose.[44] Yet another case occurred in mid-1969 when AC-130s were diverted from Commando Hunt interdiction action and AC-47 were shifted from operations in South Vietnam to counter North Vietnamese and Pathet Lao attacks on Lima Site bases used by friendly forces in northern Laos. Both ground and air observers credited the gunships with going far to frustrate the attackers, but it was hard to quantify. Yet, in the end, it was also shown that interdiction, too, was hard to quantify with any accuracy. In April 1971, the Air Staff told Air Force

commanders in Southeast Asia that there was concern over the accuracy of bomb damage assessment (BDA):

> Seventh Air Force is really concerned about the validity of the BDA reported by the AC-130 gunships in their truck-killing operations. They stated all aircraft BDA for this hunting season indicates over 20,000 trucks destroyed or damaged to date, and if intelligence figures are correct, North Vietnam should be out of rolling stock. The trucks continue to roll however.

In May 1971, Seventh Air Force Commander General Lucius D. Clay, Jr., had tests run at Tan Son Nhut Air Base which showed that a direct hit from an AC-130 had left one truck immediately operable with several others needing only limited repair.[46] What had started out as a program with clearly beneficial consequences was turned into one with results that were limited, ambiguous, and misleading.

Interdiction and "Sending Messages."

The effort to interdict supplies going from North Vietnam to support the war south of the demilitarized zone (DMZ) became caught in the toils of concern over showing American resolve. A salient case was the effort to destroy the Thanh Hoa and Paul Doumer bridges, the later on the outskirts of Hanoi and the former some 70 miles to the south. Although General Westmoreland believed air power would have been better used "by supporting ARVN operations and by hitting the enemy's infiltration route through Laos,"[47] the task of interdiction near the source went forward. But difficulties abounded, and benefits were suspect. Early on, when the Thanh Hoa Bridge was weakly defended, an F-100 flak suppressor and an RF-101 were lost in the first attack, three F-105s in the second, and one F-105 in the third (all being Air Force missions). By May 1966, defenses at the bridge had hardened with more SAM sites and more frequent MiG activity in the area. On May 31, a C-130 departed from its base never to be seen again and one F-4 aircraft was lost. The longer the bridge remained

undestroyed, the more it came to symbolize the limits of U.S. capabilities—and so, too, the more its destruction became more a psychological than a military matter. The destruction of the bridges became necessary to meet several different concerns—showing American resolve, "sending messages" to the government in Hanoi and its operatives, and defending a self-image of competence within the U.S. military. But what message was really sent? Was it that technology can eventually be brought to bear to solve all problems, or that the United States might be counted on to complete tasks at costs too high for their value? The risk was that "victory" would be Pyrrhic.

But the results of interdiction even where General Westmoreland thought it should be attempted were also disputed. Brigadier General Soutchay Vongsavanh of the Royal Laotian Army, writing in 1981, concluded that "despite the full weight of American bombing operations, Ho Chi Minh Trail truck traffic increased day by day and the NVA continued to improve the road network, keeping passages open and making roads suitable for high-speed traffic."[48] The Sihanouk Trail through Cambodia was improved at the same time. On top of this, the U.S. air effort pushed the communists farther into Cambodia, accelerating its political destabilization and, in essence, spreading insurgents rather than containing and destroying them.

As with other aspects of the war, the completion of a task testified only to the efficiency of service personnel—not to the effectiveness of the completed task. Were there times when it would have been preferable for America's "can do" military to have taken a "won't try" stance?

Airmobility.

Even some tasks that could clearly be accomplished did not have equally clear beneficial consequence. Some distinguished Americans sought relief from the war's frustrations by seeking to change the Army to a significant

degree. General James A. Van Fleet, for example, called for greater airlift capability, "compensating for lack of numbers and firepower through increased mobility and concentrated shock action." In essence, Van Fleet wanted to rely more on large special forces units.[49]

But others were less sanguine. General Robert R. Williams later reflected: "I guess it's really a question of the American way of fighting." Williams recalled evidence that overflights by helicopters were no counter to Viet Cong presence in villages. Even if one drove the Viet Cong away with air power, how long would they stay away unless men on the ground forced them? "You have to fight it down in the muck and the mud at night, and on a day-to-day basis," General Williams said. "That's not the American way and you are not going to get the American soldier to fight that way." For observers such as General Williams, reliance on technology was "the best way to go, short of reversion to true, massive, dirty, low-down guerrilla warfare."[50] Were the conditions of the war itself, then, the primary determinant of the approach to be taken to tactics, technology, and strategy? Or was it the American temperament?

CONCLUSION

Although willing to accept the occasional tactical gain, all the North Vietnamese and Viet Cong really needed to accomplish while U.S. forces remained in Vietnam was to avoid catastrophic loss while ensuring political instability throughout the south. By contrast, the United States and its South Vietnamese allies needed an affirmative victory that would produce lasting change on the ground, replacing conflict and terror with a cooperative political and social order. The political weaknesses of the Saigon government added to the Johnson Administration's sense of crisis in 1964 and 1965. But, as CIA Director John McCone told President Lyndon Johnson, it might well be a problem with no solution. On April 2, 1965, he wrote to the President:

> I have reported that the strikes to date have not caused a change in the North Vietnamese policy of directing Viet Cong insurgency, infiltrating cadres and supplying material. If anything, the strikes to date have hardened their attitude.
>
> With the passage of each day and week we can expect increasing pressure to stop the bombing will come from various elements of the American public, from the press, the United Nations and world opinion. Therefore time will run against us in this operation and I think the North Vietnamese are counting on this.
>
> What we are doing is starting on a track which involves ground operations which in all probability will have limited effectiveness against guerrillas, although admittedly will restrain some Viet Cong advances. However, we can expect requirements for an ever-increasing commitment of U.S. personnel without materially improving the chances of victory.
>
> In effect, we will find ourselves mired down in combat in the jungle in a military effort that we cannot win and from which we will have extreme difficulty extracting ourselves.

The asymmetrical "superiorities" of the American side actually carried with them certain enlarged vulnerabilities, and not the least of these was the chance of becoming "trapped by success." The ability to carry out tasks eclipsed the difficulty in demonstrating their worth. Unwilling to lose an ally, even an admittedly weak one, the U.S. government took increasing control of a war it could not win, using its asymmetrical air power edge in ways that delayed but did not change the final outcome.

ENDNOTES

1. Specific aspects of the Vietnam War addressed in this paper are covered more fully in Donald J. Mrozek, *Air Power and the Ground War in Vietnam*, Maxwell AFB, AL: Air University Press, 1988 (Washington, DC: GPO, 1988). Also, for an important appraisal of the air war especially with regard to bombing, see Mark Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*, New York, NY: Free Press, 1989. Also see Andrew F. Krepinevich, *The Army and Vietnam*, Baltimore, MD: Johns Hopkins University Press, 1986.

2. Russell F. Weigley, *The American Way of War*, Bloomington, IN: Indiana University Press, 1977 (New York: Macmillan, 1973), p. 67. Also see John K. Mahon, *History of the Second Seminole War, 1835-1842*, Gainesville, FL: University of Florida Press, 1967; Francis P. Prucha, *Sword of the Republic: The United States Army on the Frontier, 1783-1846*, New York, NY: Macmillan, 1969.

3. Weigley, *The American Way of War*, p. 68.

4. *Ibid*., Prucha, *Sword of the Republic*.

5. See K. Jack Bauer, *The Mexican War, 1846-1848*, New York: Macmillan, 1974.

6. See, for example, Robert M. Utley, *Frontiersmen in Blue: The United States Army and the Indian, 1848-1865*, New York, NY: Macmillan, 1967.

7. For present purposes, the controversial ethical implications of the term "annihilation" are not the point so much as the tendency to apply an approach to war developed in the American Civil War to circumstances little resembling that war.

8. See Weigley, *The American Way of War*, pp. 153-163.

9. See, for example, Odie B. Faulk, *The Geronimo Campaign*, New York, NY: Oxford University Press, 1969. As Weigley observes, "the lessons about guerrilla war learned by General Crook were of the kind that seemingly have to be learned anew with each American experience in guerrilla warfare." Weigley, *The American Way of War*, p. 502, n. 16.

10. See Russell F. Weigley, *History of the United States Army*, New York, NY: Macmillan, 1967, pp. 307-308; also, Frederick Funston, *Memories of Two Wars: Cuban and Philippine Experiences*, New York, NY: Scribner, 1914. Also see R. Ernest Dupuy, *The Little Wars of the United States*, New York, NY: Hawthorn Books, 1968, which includes an extended comment on operations on Mindanao.

11. U.S. officials, both civilian and military, often expressed frustration during the Vietnam War that they seemed unable to handle an obviously inferior enemy. The derisive characterization of the enemy, both Viet Cong and North Vietnamese, reveals a key "universalist" error—looking too much to quantitative measurements of what the enemy owns rather than to qualitative appreciations of how the enemy operates, what the enemy is seeking to do, and how well the former serves the latter. To Americans of the 1990s, the notion that a small, poorly armed, but thoughtfully directed force can do enormous damage

to a country superior by all conventional measurements has become highly credible. But in the 1960s, it was a thought almost impossible for high-ranking leaders to entertain.In essence, opponents so limited in their economic and social development as to invite the description "pre-modern" were more vexing than those expected to fight along "modern" lines. Thus, although the Warsaw Pact threats to NATO interests posed the risk of much greater losses than did the threats posed by the Viet Cong and the North Vietnamese, the challenge from the Warsaw Pact was much easier to understand in concrete military terms than was the Viet Cong and North Vietnamese challenge and, as a result, was easier to plan for. In the 1990s, with the disappearance of the Cold War confrontation, a "post-modern" tendency to *dis*-order, *dis*-unity, *dis*-junction, and *dis*-continuity has grown strong. In this sense, it is the success of the West in the Cold War that prepared the scene for the increasing importance of local and regional conflict.

12. The idea that war might be self-limiting under various conditions was not entirely new. For example, Raymond Aron developed this idea with respect to World War I in *The Century of Total War*, Boston, MA: Beacon Press, 1955. War became more possible, he suggested, because pre-war forecasts put consumption rates in a war far ahead of replacement rates. Thus, the war would have to end soon, one way or another, if only because the combatants would run out of the wherewithal for continuing it. Aron refers to the unexpectedly high rates of industrial production that allowed sustainment of the conflict as "technical surprise."

13. The demoralization that an enemy is expected to experience is not merely some emotional state brought on by fatigue and disappointment. It is a recognition of basic objective conditions through which one's enemy is brought to see the limits of what his power can do, no matter how long or how much it is applied. In essence, the enemy is brought to a different understanding of what strategies are possible and what tactics are useful by being converted to a different understanding of the objective conditions in the theater of operations. Concerning Mao's thoughts on warfare, see especially his "Problems of Strategy in Guerrilla War Against Japan", May 1938, and "On Protracted War," May 1938, in *Selected Military Writings of Mao Tse-tung*, Peking: Foreign Languages Press, 1968.

14. Frantz Fanon, *The Wretched of the Earth*, New York, NY: Grove Press, 1965.

15. Alistair Horne, *A Savage War of Peace: Algeria, 1954-1962*, London: Macmillan, 1977, studies the Algerian war of resistance against the French comprehensively and in detail.

16. The military defeat of an enemy, for example, need not change the mind and will of the enemy, especially over the long run. But a military occupation during which key political, social, and economic institutions are transformed can do so.

17. It is also of some importance that air power theorists often held rather concrete ideas about how "human nature" would react to devastation wrought from the air. In this way, the Americans in Rolling Thunder were not entirely different from Giulio Douhet, the latter presuming to know how all civilians would act under air assault and the former presuming to know what the North Vietnamese valued most and what sacrifices they might make to save it. The risk of projecting one's own values as if they were universally applicable is obvious.

18. The commitment to independence among Vietnamese is a central subject in Bernard Fall, *The Two Viet-Nams: A Political and Military Analysis*, New York, NY: Praeger, 1967; and in James P. Harrison, *The Endless War: Fifty Years of Struggle in Vietnam*, New York, NY: Free Press, 1982.

19. The issue of motivation among nationalist insurgents is important not only in its anti-colonialist form but in resistance to historic hegemonic forces, as in Vietnamese concern about Chinese designs in Southeast Asia. As to motive, see William Darryl Henderson, *Why the Viet Cong Fought: A Study of Motivation and Control in a Modern Army in Combat*, Westport, CT: Greenwood Press, 1979. Also see Truong Nhu Tang, *A Viet Cong Memoir*, San Diego, CA: Harcourt Brace Jovanovich, 1985.

20. Walt Rostow, "Guerrilla Warfare in the Underdeveloped Areas," speech at U.S. Army Special Warfare School, Fort Bragg, NC, June 28, 1961, Army 1961 folder, Departments and Agencies Files, President's Office Files, John F. Kennedy Papers, Kennedy Presidential Library.

21. William C. Westmoreland, *Report on the War in Vietnam as of 30 June 1968*, sec. 2, Report on Operations in South Vietnam January 1964-June 1968, Washington, DC: U.S. Government Printing Office, 1968, pp. 89-91.

22. By the late 1960s and early 1970s, U.S. leaders increasingly suggested that the Viet Cong had always been creatures of Hanoi. But they also widely subscribed to the view that Hanoi had ordered the Tet Offensive of 1968 in large part so that indigenous resistance leaders in South Vietnam could be wiped out by the Americans and by ARVN, thus leaving Hanoi in undisputed political leadership in the war against the United States and South Vietnam. Of course, if they had always been

Hanoi's creatures, what need would there have been to create an occasion for their decimation at the hands of the United States and ARVN?

23. Making political hay out of mere survival has occurred often. The Americans did it during the War for American Independence, and Saddam Hussein did it in Iraq in the 1990s.

24. See Harry G. Summers, Jr., *On Strategy: The Vietnam War in Context*, Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1981.

25. Note, too, that the introduction of large North Vietnamese units into South Vietnam came after the Saigon government had been largely deligitimized. By contrast, even allowing for earlier North Korean irregular action in South Korea, the attack by the North Korean People's Army in June 1950 was both unambiguous and notorious, providing so blunt a challenge as to preclude mere piecemeal and gradualist responses.

26. Several important advantages derived from U.S. air assets that are relevant to the issue of asymmetry will not be discussed here but may be explored in such works as Earl H. Tilford, Jr., *Search and Rescue in Southeast Asia, 1961-1975*, Washington, DC: Office of Air Force History, 1980; and Spurgeon Neal, *Medical Support of the U.S. Army in Vietnam*, Washington, DC: Department of the Army, 1975.

27. It should be noted, however, that the introduction of the Soviet-made SA-7 heat-seaking surface-to-air missiles (SAMs) made much less secure the use of helicopters for such purposes as movement of troops. Recalling his experience as an Army adviser, Stuart Herrington claimed that the missiles "changed overnight the ground rules for the use of the helicopter." See Herrington, *Silence Was A Weapon, The Vietnam War in the Villages*, Novato, CA: Presidio Press, 1982, p. 30.In addition, there was a significant challenge from MiGs in high-value areas of the North, although the claim of general U.S. air superiority still holds. Also, some exponents of air power denied that "true" air power was used in the war with the possible exception of Linebacker II. According to this interpretation, excessive distribution of responsibilities and fragmentation of authority compromised the effectiveness of the air assets dedicated to the war effort so that the synergistic effect expected from "true" air power was consistently lacking. Rather than having the parts of the air effort become greater than their sum, they became less.

28. Bernard C. Nalty, *Air Power and the Fight for Khe Sanh*, Washington, DC: Office of Air Force History, 1973, p. 21.

29. *Ibid.*, p. 19.

30. Westmoreland quoted in *Ibid.*, p. 90.

31. William C. Westmoreland, *A Soldier Reports*, Garden City, NY: Doubleday and Co., 1976, p. 204.

32. William C. Westmoreland, *Report on the War in Vietnam, as of 30 June 1968*, sec. 2, "Report on Operations in South Vietnam, January 1964-June 1968," Washington, DC: Department of the Army, 1974, p. 191.

33. Senate, Committee on Armed Services and Subcommittee on Department of Defense, Committee on Appropriations, *Hearings, Military Procurement Authorizations for Fiscal Year 1968*, 90th Cong., 1st sess., testimony of Gen. Harold K. Johnson, January 31, 1967, p. 577.

34. Moyers S. Shore III, *The Battle for Khe Sanh*, Washington, DC: Headquarters U.S. Marine Corps, 1969, pp. 110-111.

35. Westmoreland, *A Soldier Reports*, p. 412.

36. Peter B. Mersky and Norman Polmar, *The Naval War in Vietnam*, Annapolis, MD: Nautical and Aviation Publishing Co. of America, 1981, p. 141.

37. In fact, Westmoreland's commentary on the Vietnam War suggests that he only considered it to be reaching the stage of genuine warfare, rather than preliminary skirmishing however deadly, not until 1967 and afterward with large unit engagements.

38. See Jack S. Ballard, *Development and Employment of Fixed-Wing Gunships, 1962-1972*, Washington, DC: Office of Air Force History, 1982.

39. See Kenneth Sams, *First Test and Combat Use of AC-47*, Hickam AFB, HI: HQ PACAF, Project Checo, December 1965.

40. Ballard, *Fixed-Wing Gunships*, pp. 20-21.

41. Quoted in Ballard, *Fixed-Wing Gunships*, p. 179.

42. *Ibid.*, pp. 106-107.

43. *Ibid.*, pp. 61-62.

44. Alan L. Gropman, *Airpower and the Airlift Evacuation of Kham Duc*, Maxwell AFB, AL: Air University, Airpower Research Institute, 1979, pp. 7-8.

45. Message quoted in Ballard, *Fixed-Wing Gunships*, p. 169.

46. Henry Zeybel, "Truck Count," *Air University Review*, Vol. 34, No.2, January-February 1983, pp. 36-45.

47. Westmoreland, *A Soldier Reports*, p. 110.

48. Soutchay Vongsavanh, *RLG Military Operations and Activities in the Laotian Panhandle*, Washington, DC: U.S. Army Center of Military History, 1981, p. 53.

49. James A. Van Fleet to Elvis J. Stahr, Jr., letter, March 26, 1962, Army 1962 folder, Departments and Agencies Files, President's Office File, Kennedy Papers, John F. Kennedy Library.

50. Interview with General Robert R. Williams, USA, conducted by Colonel Ralph J. Powell and Lieutenant Colonel Philip E. Courts, 1977, U.S. Army Military History Institute, Carlisle Barracks, PA, Oral History Series, History of Army Aviation, p. 66. It may be noted, though, that there were some serious "exceptions to the rule." See, for example, Mark Moyar, *Phoenix and the Birds of Prey: The CIA's Secret Campaign to Destroy the Viet Cong*, Annapolis, MD: Naval Institute Press, 1997.

51. Quoted in U.S. Grant Sharp, *Strategy for Defeat: Vietnam in Retrospect*, San Rafael, CA: Presidio, 1978, pp. 74-75.

52. The quoted phrase comes from David L. Anderson, *Trapped by Success: The Eisenhower Administration and Vietnam, 1953-1961*, New York, NY: Columbia University Press, 1991.

PART II: THREATS

INTRODUCTION

Lloyd J. Matthews

With the historical context thus established, we turn to Part II, dealing with various asymmetric military threats to the United States posited for the period out to the Army After Next. Perhaps the most unsettling of the six presentations is the apocalyptic vision of Mr. Robert D. Steele as portrayed in "Takedown: Targets, Tools, and Technocracy" (including a complementary piece "Information Peacekeeping: The Purest Form of War").

The gravamen of Steele's case is that the United States is susceptible to being "taken down" owing to its naked vulnerability in four categories: physical, cybernetic, data, and mind-set. Our technological apparatus has far outstripped our ability to secure it, while government and public complacency is endemic. Just as disconcerting, the details of America's vulnerability are available to all national enemies through open-source intelligence. Another complicating factor is that the matrix of information warfare in the United States—our "information commons," as Steele calls it—lies in the civil sector and is thus outside the Defense Department's traditional sphere of resource mobilization and control.

The solution according to Steele lies in new appropriations of $2 billion a year—half for electronic security and counterintelligence, half for creating a virtual intelligence community able to execute information peacekeeping operations. As described in detail in his second paper, information peacekeeping is "the active exploitation of information and information technology so as to achieve national policy objectives." It is based on the revolutionary premise that intelligence can be a virtual

substitute for such modalities as violence, capital, labor, time, and space.

From the heady realm of virtual reality, we enter the more prosaic but no less problematic world of terrorism as treated in Professor Stephen Sloan's "Terrorism and Asymmetry." Political terrorism, almost always an asymmetric form of armed conflict, has been defined in many ways, but all definitions include these two elements: (1) the threat or use of violence against a small number of immediate victims, and (2) having the purpose of coercing a larger target group through fear to accede to the political demands of the perpetrators. Against a nominally impregnable superpower like the United States, terrorism will always be the option of first resort for small desperately aggrieved groups that otherwise remain powerless and impotent. Noteworthily, possibilities of "virtual terrorism" now coming into view ally well with certain forms of information warfare to which, as we saw in Mr. Steele's presentations, the United States is becoming increasingly vulnerable.

In his cinematically imagined scenario "Five-Dimensional Warfare: Can It Defeat the Army After Next?" (not included in this volume, but published as a separate U.S. Army War College Strategic Studies Institute monograph, dated March 10, 1998), Dr. Robert J. Bunker synthesizes several elements of the likely threat environment over the next 25-plus years to conjure a plausibly competitive opponent of the U.S. BlueFor. This opponent, christened BlackFor, employs a so-called five-dimensional approach (land, sea, aerospace, temporal, and cyber) designed to exploit BlueFor weaknesses as seen emerging from the Army After Next, while exploiting BlackFor's own significant technological capabilities.

Black, born in the growing failed-state environment of the future where political power has shifted from legitimate states to mongrel political-criminal entities, is defined territorially by heavily urbanized coastal zones that cross

national boundaries and contain sprawling, densely populated slums. BlackFor is manned by members of the new warrior class. It is augmented by mercenaries, specializes in terror, and flouts such effeminacies as laws of war, rules of engagement, and public opinion.

Doctrinally and in certain technological niches such as advanced nonlethal weapons and robotics, BlackFor aims to overleap BlueFor exponentially, putting itself on a more than equal footing. Conceptual innovations deriving from five-dimensional battlespace, though smacking of *Star Wars* and *Star Trek*, are soundly based. For example, spatial expansion can occur through stealth-masking; a BlackFor soldier in civilian garb standing next to a BlueFor soldier is effectively a 1000 miles away. Spatial contraction effectively occurs, for example, when a BlackFor speed-of-light laser beam disables a BlueFor tank at long range in an instant.

The non-linear concepts and technologies that underlie BlackFor are the source of its asymmetric advantage. They may outstrip by a quantum leap the U.S. Army's present linear extrapolations into the future based upon soon-to-be outmoded Newtonian and Clausewitzian modes of thinking. If the present institutional mind-set is not overcome, according to Dr. Bunker, "it will potentially set up the Army After Next and the American public for a strategic defeat many magnitudes greater than anything ever before experienced in our nation's history."

In "Metaphors and Modern Threats: Biological, Computer, and Cognitive Viruses," Mr. Edmund M. Glabus employs the virus metaphor as a heuristic device for shedding light on three asymmetric threats to U.S. national security that might otherwise be difficult to visualize—biological warfare, computer network attack, and memetic warfare. In some forms of biological warfare, of course, viruses might be used literally as the agent of attack, but the metaphor of the spreading virus as deadly contagion is ideal for imaging forth all agents of biological

attack, the bacteria anthrax and botulism toxin being prime examples.

The metaphor of attacking computer systems through the introduction of software "viruses" is now fairly well-understood by an increasingly computer-literate American public, many of whom have confronted this exasperating phenomenon directly on their personal computers at home or work. Mr. Glabus, however, extends the metaphor to include the "infectious" and far more serious activities of hackers, who gain unauthorized access to computer networks to alter or extract information or to introduce viruses. Thus virus becomes a metaphor for cyber attacks in general, covering the entire range of potential attacks on America's computers and computer networks and systems.

Memetic warfare is the least understood and perhaps most problematic of the threats treated by Mr. Glabus. Conceptually, it lends itself well to elucidation through the viral metaphor. Think first of traditional psychological warfare, whereby the perceptions of the U.S. political leadership, populace, or military are manipulated purposefully by the enemy in ways that threaten our security. Now think of a certain subset of psychological warfare, a particularly insidious one in which the harmful perceptions are self-replicating. Copies ("memes") of the harmful perceptions are passed from one mind to another in a continuing process, so that eventually the entire group psyche is "infected." Soldiers in combat talk to one another, and when a bad idea is lodged in the mind of a few by a clever enough enemy—the nirvana of surrender and quick passage home?—the idea might multiply quickly through an army.

Though we cannot know now the extent to which memetic techniques will prove to be effective additions to the practice of psychological warfare over the next 25 years, certainly, as Mr. Glabus demonstrates, we must be alert to the developing threat. To enemies who cannot match us on

the conventional battlefields of land, sea, and aerospace, the battlefield of the psyche will be a tempting alternative. For such enemies, one good bad idea could well be worth a thousand bombs.

From asymmetrics of technology, wealth, doctrine, information, and organization—all group traits attributed generally to larger populations—Ralph Peters, in "Our New Old Enemies," descends to the level of individual asymmetry: how will our soldier sons and daughters differ from the new warriors that inhabit the enemy's ranks tomorrow? This is not an inconsequential question, for all serious study of war leads to the inescapable conclusion that the ultimate discriminator between contending forces is the character of the individual soldier.

In his sermon on the human heart, Ralph Peters explores to a level that makes us squirm the essential nature of Homo sapiens. He finds, like the author of *Genesis*, that man is fallen, that his essential nature is emblematized by the "massacre, genocide, ethnic cleansing, rape, plunder, kidnapping, assassination, ineradicable hatred, and endless warfare" that are chronicled in the Old Testament and indeed throughout secular history.

Our warrior enemies of the future—once the hopeless, the dispossessed, the alienated, now the fanatic, the zealot, the true believer with nothing to lose and all to gain—are the perfect embodiment of all the evil potential that lies at the heart of man. Our sons and daughters, fallen and imperfect like all humans but ameliorated by the balm of Western humanism, will be sent out to fight the legions of darkness. If in the name of human goodness we tie their hands unnecessarily, we risk tipping the asymmetries in favor of the enemy. In Ralph Peters' relentlessly honest vision, our sons and daughters "will still win when allowed to do so. But more of them will suffer and die for lowered returns because of our stubborn unwillingness to face the complexity of mankind."

The conference presentation by Dr. Steven Metz titled "Trans-National Threats" (not included in the present volume) addresses the general category of potential danger to U.S. security posed by enemies unaffiliated with or not confined within particular states. Glancing back to America's vulnerability on the cyber front as portrayed by Robert Steele, to certain forms of international terrorism as treated by Stephen Sloan, and to Robert Bunker's concept of coherent armies arising from particular cultural-geographic breeding grounds lying athwart established national boundaries, Dr. Metz focuses on an increasingly important slice of the total threat spectrum—transnational enemies.

Such enemies—diverse blends of political, ideological, ethnic, and religious groups, as well as criminal networks—would wage indirect warfare, often contracting out the technical dirty work, with the aims of weakening America's social fabric and disrupting its security-information infrastructure. Such means of conflict, so fundamentally different from traditional state-on-state warfare under the Westphalian system, will require profound adjustments in U.S. security philosophy.

Those who scoff at the threat of future transnational warfare might want to ponder the great interest shown in Unabomber Ted Kaczynski's anti-industrial manifesto, recently displayed on the Internet. Anarchists, antitechnologists, radical environmentalists, and other primitives were drawn to it as a bee to honey (*Scientific American*, April 1998).

TAKEDOWN:
TARGETS, TOOLS, AND TECHNOCRACY

Robert D. Steele

ABSTRACT

This paper is a "primer" which attempts to place national security and national intelligence in a larger context, one which must be understood if America is to survive and prosper at the dawn of the 21st Century. The targets are too numerous to discuss in detail, but they can be grouped into four large categories: physical, cybernetic, data, and mind-set. The tools are also too numerous to discuss in detail—tools as elementary as paperclips and pick-axes can inflict grave damage on very complex and inherently fragile systems. Of gravest concern in considering the tools available to wreak havoc on our national infrastructure is the simple fact that we remain our own worst enemy—we actively open the door to insider abuse, out-sourced code, and naked data. Our technocracy and its culture will continue to impede change. If we are to succeed in the future at our given task of defending the Nation against all enemies, "domestic and foreign," then we must redefine national security and national intelligence to focus on data and knowledge and national intelligence writ small but wide. We must fund, from within the existing budget of the Department of Defense, both the $1 billion a year for electronic security and counterintelligence oriented toward our true center of gravity, the private sector; and we must at the same time ask of the Department of Defense a matching amount, an additional $1 billion a year. This latter amount is needed to fund an extended "Virtual Intelligence Community" which comprises a new "order of battle" able to execute "Information Peacekeeping" operations at home and abroad, in order to deter and resolve conflict at the local, state, national, and regional levels.

INTRODUCTION

This is not a technical paper—there are many of those, each delving into the minutia of taking down power, financial, transportation, or general communications systems.[1] Instead, this paper seeks to provide a general overview of target categories and potentially catastrophic outcomes; a review of the range of tools by which these targets can be taken down; and a brief discussion of the technocracy and its culture which perpetuate our vulnerability to cybernetic melt-down. All this, however, is but a preamble to a larger discussion of national security and national information strategy.

In particular, the paper explores a redefinition of national security and national power. Our information "order of battle," and in particular our ability to protect and harness data in the private sector, and our ability to continue to exploit data across human generations, must be recognized as the most critical factors contributing to national security and national competitiveness. The brittleness of our existing complex systems, with multiple embedded points of failure, is the lesser vulnerability. The large vulnerability is at the data and knowledge level. Under these circumstances, "continuity of operations" takes on a whole new meaning, and indeed merits the scale of funding that once characterized the same term during the Cold War. In brief, we need to worry less about deliberate externally-sourced attacks, and much more about inherent embedded cancers of our own making. This paper reviews targets, tools, and technocracy in that larger context.

Let's begin with the following observation from a knowledgeable observer:

> As far as vulnerability in the medium term goes, it looks to me like American digital tech is taking itself down via its severe and accelerating self-obsolescence problems. The brittleness, like the underlying tech, is autocatalytic. The Y2K problem is a wholesome first sniff of the carnage to come. No enemy made all the early NASA satellite data now unreadable. We did. It's one

of those Pogo moments. This in no way depreciates the external threat, just adds another—temporal—dimension.[2]

Our nation is strong, and many rural areas can survive a meltdown, but most urban areas will not degrade gracefully. They will "crash," and in their crashing we will see tolls of dead and wounded greater than we suffered during the Vietnam war. We have to ask ourselves: are the right people in charge of national security? do we really understand the threat? do we have what it takes to change?

As we consider the targets and tools that can be used to effect a "takedown of America, we must do so in the context of a refreshed understanding of what constitutes "national security." In this regard, note Figure 1.[3]

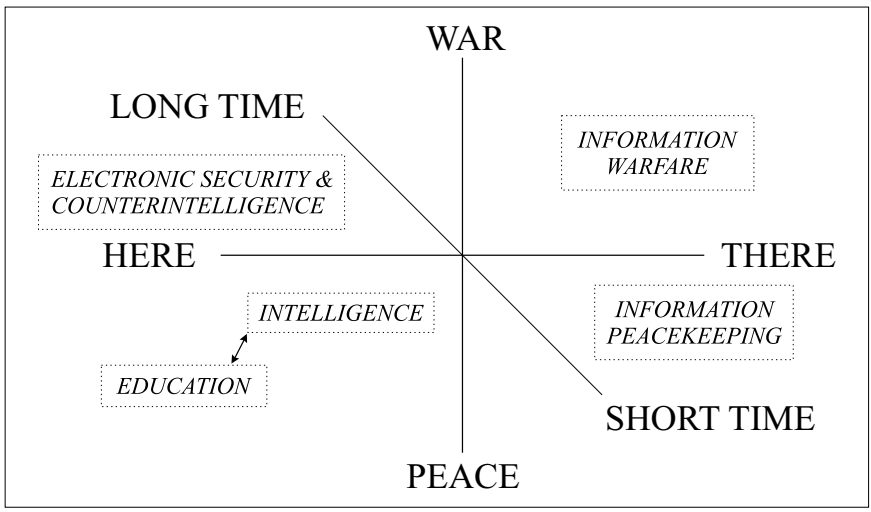

Figure 1. Redefining National Security.

This paper will not focus on the Information Warfare or Information Peacekeeping elements illustrated in the figure.[4] Instead, it will focus on the fact that the President's Commission on Critical Infrastructure Protection (PCCIP) report of October 1997, while successful in beltway terms, did not provide a credible and comprehensive threat and vulnerability assessment, a list of specific problems, statistics, and detailed case studies, and a coherent plan for

constructive change.[5] As Winn Schwartau has put it, we had the wrong people asking the wrong questions, and now we have the wrong people in charge of securing our home front—and with no real authority or money to spend.[6] Also in the classified arena, the same has been said of the National Intelligence Estimate (NIE) on the subject of U.S. vulnerabilities to information warfare attacks—with the passing comment having also been made that the author of that NIE did not know who to talk to outside of a few beltway bandits.[7] In Virginia, a well-conceived plan by a Navy admiral to sharpen his information warfare capabilities by conducting a vulnerability assessment of all systems in the state of Virginia, was set aside for fear of public reactions. The bottom line: we still don't know how vulnerable we are, and we have no idea how to go about the long-term process of creating self-healing systems rather than—as Stewart Brand aptly labels them—"self-obsoleting systems."

The "pyramid of vulnerability" for developed nations, and most especially for the United States —which owns, uses, and is severely dependent on the bulk of the communications and computing resources of the world—is illustrated in Figure 2.

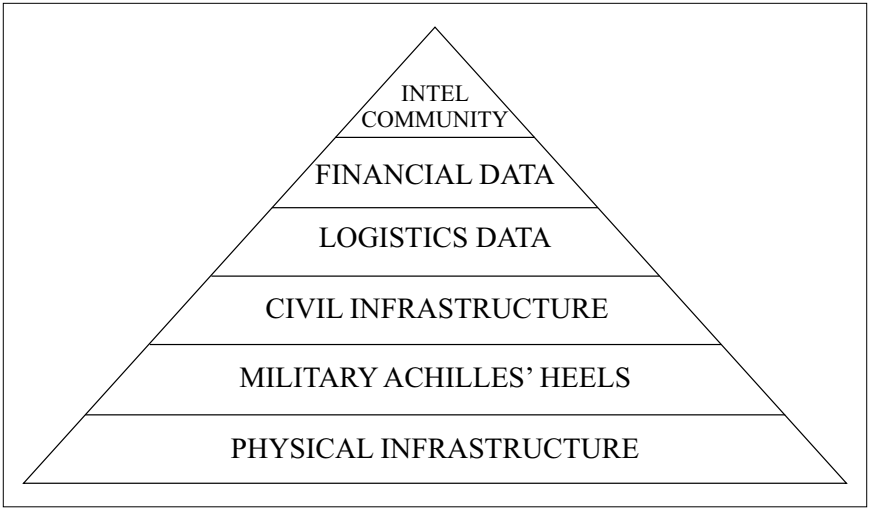

Figure 2. Pyramid of Vulnerability.

This pyramid of vulnerability seeks to distinguish between four distinct kinds of vulnerability:

1. The vulnerability of major physical infrastructure elements, such as:

- Bridges, levees, and dams—such as the 2800 readily mapped for the public of which 200 or so are of strategic consequence in isolation[8]
- Canals—such as the Panama Canal, with very vulnerable locks
- Pipelines—such as the Alaska Pipeline
- Critical railway switching points.

2. The vulnerability of obvious military Achilles' heels, as well as obvious civilian infrastructure, such as:

- Airborne Warning and Control System (AWACS) and aerial tankers (anti-tank missiles, or plastique on landing gear—tend to be concentrated in one place)
- Submarine communications antennas (e.g., Annapolis golf course)
- Charleston channel (major sealift departure area)
- Civilian power and communications nodes supporting command centers and key facilities (Falcon AFB Study, Kansas City payroll)
- Major power grid nodes (both transfer and generation)
- Major telecommunications nodes, including microwave towers.

3. The vulnerability of core data streams vital to national security and national competitiveness, such as:

- Historical, environmental, and other critical planning data
- Civilian fuel stock data
- Military logistics stock data
- Transportation status data (induce rail crashes, cripple airports)
- Financial accounts data (incapacitate procurement, induce panic, impose costs of alternative accounting)
- Financial transfers data (corrupt transfers, place international and regional transfers into grid-lock, induce panic).

4. The vulnerability of our Intelligence Community (IC) to both external attacks against its systems as well as its perceptions, and internally-perpetuated misperceptions and gaps in understanding, such as:

- Attacks against down-links (Area 58, NSA, CIA, Suitland, Bolling)
- Attacks against Joint Intelligence Centers
- Internal lack of global geo-spatial data
- Internal lack of integrated analysis model
- Internal lack of foreign language and foreign area expertise
- Internal lack of access to international experts and open sources.

In summary, this rough depiction seeks to drive home the point that a "takedown" of America is not simply a matter of electronic attacks against electronic systems, but rather a much more comprehensive range and scale of

vulnerability which encompasses everything from key geo-physical nodes to our intelligence mind-sets, and which can be attacked with a range of tools that includes: pick-axes and chain saws against selected cables; anti-tank missiles against AWACS and aerial refuelers and satellite dishes; 18-wheeler trucks with and without explosives against specific transformers or other key nodes; electrical attacks; and, finally—the area least considered today—data and mind-set attacks and self-generated vulnerabilities.

"Top Ten" lists cannot possibly capture the full extent of the nation's vulnerability, but they are a helpful means of highlighting the diversity and the imminence of our vulnerability. They can help accelerate constructive change.

TAKEDOWN: TARGETS AND TOOLS

John Perry Barlow, lyricist for the Grateful Dead and co-founder of the Electronic Frontier Foundation, once said that "the Internet interprets censorship as an outage, and routes around it."[9] Exactly the same can be said for any strategy that seeks to "harden" or protect specific nodes. Like Internet censorship, it simply will not be effective.

We are at a point in time where, as Steward Brand has noted, the Year 2000 problem is but "a wholesome first sniff of the carnage to come." Our system of systems is internally vulnerable from the first line of code on up, and externally vulnerable at every single switching point that relies on either software or electronic transfer. Figure 3 illustrates this larger discussion.

On the left of the figure, we have a column of possible targets, ranging from the process-oriented (secret decisions), down through data links and data stocks, into computers and power stations, and finally to larger physical infrastructure features which can be attacked by physical and electronic means. On the right we have a column of attack categories ranging from the mundane hand-held

instrument, passing through foreign code embedded in major U.S. systems, and culminating in the inherent weaknesses of our national electronic engineering training and our existing decision mind-sets.

• HUMAN DECISIONS	• EXISTING MIND-SETS
• IC DOWNLINKS	• EXISTING EE SKILLS
• FEDERAL RESERVE	• CALCUTTA CODE
• FUEL STOCK DATA	• PAID INSIDERS
• DATA COMPUTERS	• ANGRY INSIDERS
• POWER TRANSFORMERS	• INFO-MAURADERS
• CULPEPPER SWITCH	• RANDOM VIRUSES
• CINCINNATI RAIL YARDS	• 18-WHEELERS
• ALASKA PIPELINE	• PICK-AXES/BACK-HOES
• BRIDGES, LEVEES, DAMS	• MOTHER NATURE

Figure 3. Targets and Tools for Taking Down America.

Representative Targets.

*Bridges, Levees and Dam*s. In the United States, the Mississippi and Missouri Rivers, natural wonders in their own right, are also natural obstacles of monumental proportions. There are exactly six mainstream railway bridges across these great rivers, across which the vast majority of U.S. grains must go from the plains to the East Coast cities, and the vast majority of manufactured goods must in return go from the Northeast and the South. As the natural flooding in 1993 demonstrated,[10] when these bridges are closed, whether by accident or intent, there are severe repercussions for trade, and especially for the stockage of food and fuel. Recent breaks in levees in the South have demonstrated our vulnerability to the assumption that man can contain nature without regard to human attack. This bears emphasis: all insurance and risk calculations today assume natural causes of disaster. There are no calculations for risk and damage associated with deliberate human attack of any normal civil structure. Dams, in contrast, present computer controlled physical

infrastructures which can be taken over either to release flood waters, or to avoid the release of flood waters with the intent of weakening if not destroying the dam.

Alaska Pipeline. This pipeline, going across vast stretches of unoccupied territory, carries 10 percent of the domestic oil for the United States.[11]

*Cincinnati Rail Yard*s. As of 3 years ago, and very likely still today, the entire East-West railway architecture depended on exactly one major turnstile for redirecting railcars. It is located in the Three Rivers area, and represents a significant vulnerability.[12]

Culpepper Switch. A lucrative target, this simply represents the kind of critical communications node (voice and data, especially financial and logistics data) that can be attacked in both physical and electronic ways. The Internet has various equivalent nodes, two of which merit special attention—MAYEAST and MAYWEST. Taking out MAYEAST disconnects the U.S. government from the rest of the Internet world, and not incidentally does terrible things to all of the Wall Street capitalists who are "tunneling" their Intranets across the larger Internet.

Power Generators. Power generators and the grids they support can be browned out, burned out, and confused. Altering the computer readings can cause them to draw more power than they can handle, or less power than they need. Burning out the generators or melting core lines creates the interesting challenge of replacement in the absence of mainstream power. There are exactly 18 main power transformers that tie together the entire U.S. grid, and we have only one—perhaps two—generators in storage. Interestingly, all of these come from Germany, where there is a 6- to 18-months waiting period for filling orders—assuming the German generators have not been burned out at the same time by someone attacking the Western powers in a transatlantic cyber-war.[13]

Data Computers. Any computer holding large quantities of critical data, especially parts inventories and data associated with either the transfer of funds or the operational effectiveness of critical equipment, is vulnerable to data distortion—this is a far more insidious and dangerous problem than the more obvious denial and destruction attacks.

Fuel Stock Data. Fuel stock data are isolated because of their implications in terms of overloading large tanks, with the fire storm hazards of large spillage, or of failing to channel fuels because of false readings.

Federal Reserve. Until a couple of years ago there were 12 regional computing centers, one for each of the Federal Reserve regions. Then we went to a single national system with a single hot back-up computing system, and an additional cold back-up alternative.

IC Downlinks. Past surveys have focused on buildings, but the more capable attackers will focus on downlinks. All of the main satellite downlinks—for NSA, CIA, Area 58, key other government departments, are out in public sight and reachable with a hand-held anti-tank missile fired from outside the fence line.

Human Decisions. "We have met the enemy, and he is us." This often quoted line from Pogo is complemented by another observation, this one anonymous, to wit, "A nation's best defense is an educated citizenry." This "target" is listed to bring out both a vulnerability and an opportunity for "hardening" our national defense. Just as "commander's intent" is used in planning for complex operations where communications may be lost, it is essential that there be a larger national decision-making architecture in which there are few secrets and the public is fully engaged. In this way, when disasters do happen and many communications channels do break down, the public will be less likely to panic and more likely to use common sense and good will to see the crisis through. A thorough public understanding of our vulnerabilities and our plans for dealing with those

vulnerabilities is essential to our progress. This "target" is also intended to make the point that the weakest link in all systems is not the system itself, but the humans associated with the system.

Representative Tools.

Pick-Axes and Back-Hoes. Paperclips have burned out strategic warning computers. Pick-axes can cut critical cables in strange places that are difficult to discover. Back-hoes easily take out cables—perhaps the most famous, popularized by Winn Schwartau, is the back-hoe that took out Newark Airport's primary communications and air traffic control and also—right there running alongside it, the "redundant" cable intended to serve as a back-up for the primary cable. Across America, at every cable crossing, we post large signs saying in essence, "Cut Here."

Eighteen Wheelers. Eighteen wheelers, whether or not loaded with explosives, are a useful intellectual construct. Any critical node should be subject to the 18-wheeler test—what will happen if an 18-wheeler crashes through at full weight and speed at any one of various points; or alternatively, what will happen if an 18-wheeler "melts down" at a specific point and needs to be taken apart or lifted out piece by piece?

Random Viruses. The recent spate of Windows-NT melt-downs is simply another step down the path started by the Robert Morris virus a decade ago. This situation needs to be taken very seriously because many of the viruses are encased in shrink-wrapped hardware and software coming directly from the production facilities.[14] Until software is self-healing (and code is encrypted at levels above what is presently available), this will continue to be a serious vulnerability. All of the problem tool areas discussed below will exacerbate this situation.

Info-Marauders. As has been noted by one prominent wag in this area, "hacker tools are now in the hands of idiots and criminals."[15] A single individual, empowered by hacking software freely available on the Internet, is now able to cause the kind of damage to corporate and national systems that was previously in the province only of Great Nations. Disgruntled, dishonest, crazy, and zealot individuals and gangs are now is a position to damage data, deny access, and extort funds from hapless system owners who did not realize that they were buying into a "naked Emperor" environment.

Angry Insiders. The losses to external penetrations and externally sourced viruses are much over-rated. As Dr. Mich Kabay, Director of Education for the International Computer Security Association (ICSA), has noted in his seminal work on computer losses,[16] the largest losses after fire and water problems are caused by *insiders*—dishonest or paid insiders (roughly 10 percent) and angry insiders seeking revenge (roughly 9 percent). These are people with authorized access who are able to do unauthorized things that are not detected because the systems are all designed under the assumption that insiders can be controlled through a few simple (and often very poorly administered) control measures.

Paid Insiders. Paid insiders can be simply dishonest employees who seek to exploit access for financial gain, or insiders who have been recruited by outsiders for a price. There are also former insiders who return to their place of employment (e.g., selected Wall Street firms with marginal physical access controls and worse computer access controls) to take internal actions that are not authorized and for which authorized access has expired administratively but not technically.

Calcutta Code. Also called Moscow code, this refers to computer code written by the legions of off-shore coding houses. Computer code in the United States is notorious for its lack of documentation, with the result that older systems

tend to have millions and millions of lines of code that are completely incomprehensible even to the most skilled examiner, and replete with patches from a variety of sources, all also undocumented. As the Year 2000 problem takes on greater urgency, many organizations are being forced to provide intimate access to their code for legions of external programmers, generally without any assurance at all as to their criminal and psychological history, and also without any ability to audit their access or their code.[17]

Existing EE Skills. Our electrical engineering education is abysmal, despite the wealth of opportunity in the field and the shortage of skilled professionals. For reasons that escape the author, the electrical engineering discipline decided to completely ignore electronic security and counterintelligence issues after the demise of the mainframe (and even those standards were mediocre). Entire complex systems have been built from the ground up without any embedded security at all. In fact, some systems require or choose to turn off those rare security features provided in some software and hardware. Until national legislation establishes "due diligence" standards for the protection of intellectual property, communications, and computing products and services, this severe and pervasive vulnerability will prevent any substantial success in hardening individual targets or constraining the utility of other attack tools.

Existing Mind-Sets. Winn Schwartau, author of *Information Warfare: Chaos on the Electronic Superhighway,*[18] deserves full credit for bringing this situation before the public. Without his efforts, it is highly unlikely that the PCCIP would have been created. Its report has many flaws and oversights, to include a lack of understanding of the valid and useful perspectives of international authorities as well as the hacker underground, but it is a good start and we are in agreement on one important fact: $1 billion a year is needed to create a survivable electronic environment. This is the amount the author proposed in 1994 in testimony to the National Information Infrastructure working group.[19]

Unfortunately, the U.S. government continues to drag its feet in bringing order and security to cyberspace. This has been cited by many in the private sector as the reason they continue to ignore computer security issues.[20.]

TECHNOCRACY

This brings us to the technocracy. Figure 4 is an authoritative depiction of the sources of damage to computer systems and data. Although the originator, Dr. Mich Kabay, likes to use the words "rough guesses" with this chart, it is as authoritative as any major study anywhere, and should be carefully considered in that light.

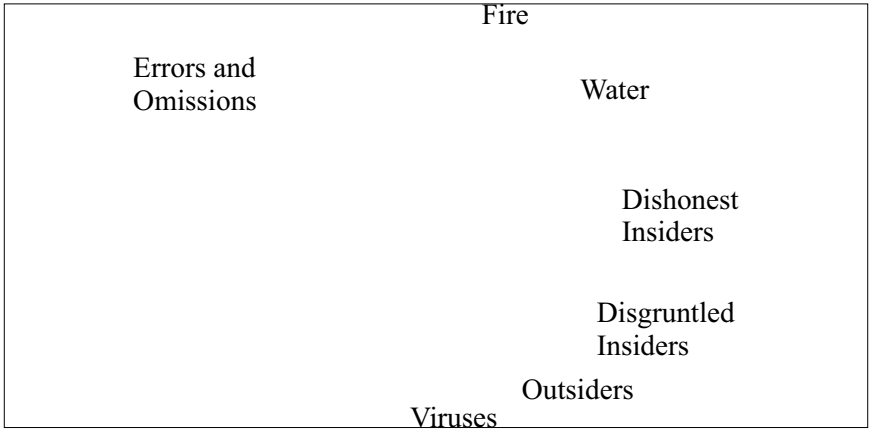

Figure 4. Estimated Sources of Damage to Computer Systems and Data.

The bottom line here is that fully 70 percent of our losses can be attributed to poor design—poor data entry and data management programs that induce major errors and omissions (and that cannot audit or flag possible errors and omissions in passing) and poor system design and system back-up practices that permit fire and water to wreak irreversible damage to important data. Only the last 30 percent have anything to do with humans. *Insiders* do roughly 20 percent of the damages. Roughly 5 percent of the

remaining damages are done by outsiders, and a final 5 percent by viruses from various sources.

In the immortal words of Robert Stratton, one of the most capable of international hackers (and one of the few never to be indicted or considered for indictment), "If houses were built like computers, the first woodpecker to come along would bring down civilization."[21]

The technocracy—the culture of technocracy—is the major impediment to change today, and we now know that all the money in the world is not going to heal our rapidly atrophying system of systems unless we first come to grips with the intellectual cancer that permeates this element of our society—which is at once so very important, but also so very dangerously vulnerable.

Among the sins of the technocracy are the following:

1. Blind faith in technology

2. No legal liability for failure (by permission of Congress)

3. No requirement for inherent security at the code and data level

4. No requirement for data integrity and survivability

5. Marginal adherence to existing back-up and access control standards

6. Elitist (largely ignorant) attitude about cryptography and privacy

7. History of ignoring detailed warnings

8. Recent record of lip service and tail chasing.

The point is that both the people and their government must accept responsibility for designing and protecting the future system of systems upon which every aspect of national security and national competitiveness must depend. It is we as individuals, willing to accept self-obsoleting technology with built-in hazards to our data,

who have permitted this gross externally imposed diseconomy to persist, and it is we the people—not the profit-taking beltway bandit creators of these systems—who will ultimately pay the final price for failure: individual poverty, scattered catastrophe, and national weakness.

The PCCIP was at once a small sign of hope and a large symbol of despair. It did not talk to any of the serious professionals outside the beltway, and even more so, outside the nation, professionals who actually know in detail the vulnerabilities and solutions the Commission was supposed to address. The PCCIP also neglected to provide the public and the private sector with an authoritative unclassified work that addresses the critical issues of data integrity, data privacy, and the use of unencumbered encryption in order to secure electronic commerce. No doubt the PCCIP marched to its secret drummer and gave its masters exactly what they *wanted*—unfortunately, it did not give the nation what it *needed*, and we are left—as we were left in the aftermath of the Report of the Commission on the Roles and Capabilities of the United States Intelligence Community—with no clear-cut direction, no one clearly in charge, and no basis on which to mobilize the private sector as the first line of national defense against cyber-attack and self-destructive electronic systems.

CIVIL CENTER OF GRAVITY

Apart from the failings of the technocracy, there is another element that makes it difficult for America to secure her computing foundation from attack— the fact that the vast bulk of the critical data and the critical electronic pathways and storage facilities are all in the private sector. It is literally impossible for the government to control and protect the most vital targets in traditional ways, nor is it even possible for the government to regulate this arena in detail. This is why the PCCIP—for all of its good intentions—must be regarded as a distraction if not a

failure. It did not address the threat or the solution in terms that could be executed by the ultimate responsible party, the private sector and the public.

Every aspect of Information Operations—from offensive information warfare to proactive Information Peacekeeping;[22] from electronic security and counter-intelligence to protect intellectual property on the home front to education as the foundation for a truly "national" intelligence community—the "center of gravity" is solidly within the "information commons" defined and dominated by the private sector. In this regard, see Figure 5. The Department of Defense cannot defend this critical terrain—nor should it—using traditional methods.

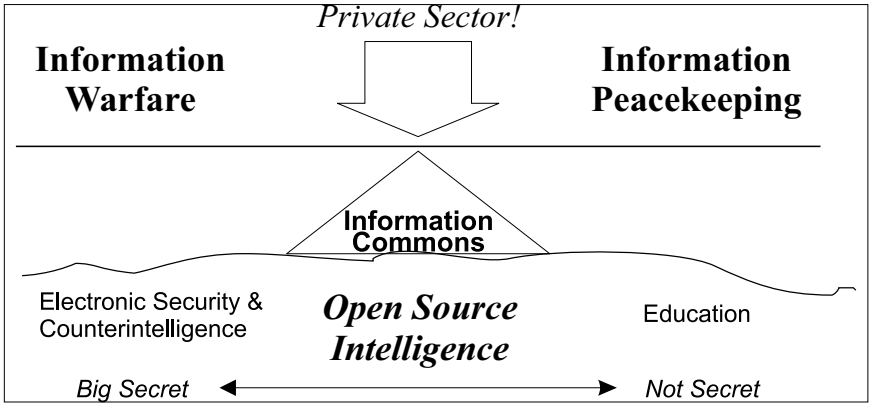

Figure 5. Civil Sector Center of Gravity.

In contemplating the takedown of America, and in considering a few representative targets and tools as well as the technocracy that spawned our pervasive national vulnerability to information apocalypse, we are forced to acknowledge that America has passed from one world to the next—from the physical world to the virtual world—and this requires that America's concepts of national defense and government operations all be subject to sharp and urgent redefinition.

VIRTUAL INTELLIGENCE AND INFORMATION PEACKEEPING

Several points regarding these two topics are worth highlighting:

1. Roughly 80 percent of what we need to know to defend the nation is in the private sector, presently outside of federal control. Roughly 95 percent of what we need to know to assure national competitiveness is in the private sector, again beyond federal control.

2. The greatest obstacle our government faces today in assuring national security and national competitiveness—the cause of causes for conflict and economic loss—is the growing gap between those with power and those with knowledge.

3. Our concept of information operations must—absolutely must—come to grips with this reality. Information warfare and electronic security and counterintelligence are anemic if not counterproductive endeavors if they are taking place in isolation from this larger construct.

4. In order to be effective in the 21st century, especially during the first half of the century when we continue to live in the largest of glass houses and our enemies—be they individuals, gangs, corporations, or states—have the most rocks, we must adopt three concepts as fundamental to our national security:

a. National intelligence must evolve rapidly to become the core of a larger "virtual intelligence community" in which we are able to fully harness and exploit private sector data from multi-lingual sources.

b. Electronic security and counterintelligence must become pervasive; this is possible only if we release the private sector from artificial constraints on encryption, and if we return to our democratic foundation, the respect for

personal privacy. We cannot regulate this arena; we can only nurture this fundamental national security principle.

c. Information peacekeeping must become our first line of defense in dealing with enemies both domestic and foreign. This will require new concepts and doctrines, a completely new order of battle, new relations between elements of the government and between the government and the private sector, and—most importantly—a completely new attitude about how to deal with such problems and threats.

5. All of the above—the full integration of a national electronic security and counterintelligence capability which protects and harnesses down to the data and code level—requires a national information strategy and a reconstruction of the administrative, legal, financial, and operational relationships among civilian, military, and law enforcement elements of government. Once we have our own act together, then we can contemplate setting standards and requesting collaboration in kind from other states.

CONCLUSION

We are at war today. It is a total war, yet we have failed to mobilize the nation, and we have therefore left ourselves without sanctuary, without a defendable rear area, and without any plan for recovering from the catastrophic consequences that can be brought about so very easily by individuals, gangs, or other nations who choose to hurt us where we are least able to respond.

Everything we are doing today, from the PCCIP to the Information Operations activity at Fort Meade to the billions of dollars being spent on the current and planned force structure, ignores the reality that pioneers Alvin Toffler, Martin Libicki, and Winn Schwartau have been trying to articulate. It is out of touch with the reality that Eric Bloodaxe, Emmanuel, Phiber Optic, Dark Angel, Andy

Mueller-Maguhn and others have been actively demonstrating. It is out of touch with the efforts of Marc Rotenberg, David Banisar, and others associated with responsible computing. Sadly, it is also out of touch with the American people and with the global community that actively seeks open intellectual engagement with responsible electronic security.

Today, the United States is again an unbalanced giant, again a paper tiger, again at the mercy of forces it does not understand and is not willing to engage in unconventional ways. We have seen the enemy, and he is us (Figure 6).

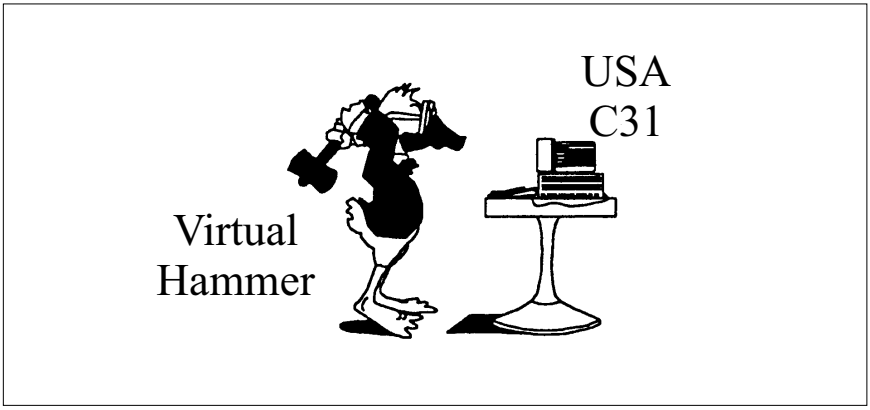

Figure 6. We Have Seen the Enemy, and He Is Us.

There is, however, good news. The price tag for all of this is authoritatively estimated at $2 billion a year (half for electronic security and counterintelligence, half for creating the virtual intelligence community able to execute information peacekeeping operations).[23.] This is a price that DoD can afford to pay, and a price that—if paid by DoD—will permit us to reinvent the concept of national defense, deter cyber-war, and surprise friends and enemies alike with our ability to adapt to the chaotic environment we have ourselves created. DoD can solve this problem, but only if it pays up, and lets go.

ENDNOTES

1. Although other papers have been written since, the three "originals" are Major Gerald R. Hust, "Taking Down Telecommunications," School of Advanced Airpower Studies, 1993; Major Thomas E. Griffith, Jr., "Strategic Attack of National Electrical Systems," School of Advanced Airpower Studies, 1994; and H. D. Arnold, J. Hukill, and A. Cameron, "Targeting Financial Systems as Centers of Gravity: 'Low Intensity' to 'No Intensity' Conflict," *Defense Analysis,* Vol. 10, No. 2, 1994, pp. 181-208. See also Robert D. Steele, "The Military Perspective on Information Warfare: Apocalypse Now," Speech to the Second International Conference on Information Warfare: Chaos on the Electronic Superhighway, Montreal, January 19, 1995; and http://www.infowar.com. The *Proceedings* of the InfoWarCon series can still be obtained from the International Computer Security Association. The author's first call for $1 billion a year for electronic security was published as a U.S. Newswire press release on August 11, 1994. Two other papers deserve mention up front: Major Roger Thrasher, *Information Warfare: Implications for Forging the Tools*, Naval Postgraduate School, June 1996; and—dealing with the tough issues of what constitutes an attack, what the legal authorities are for retaliation, and what constitutes proper retaliation—Commander 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),* Naval War College, June 14, 1996.

2. Stewart Brand was the founder of both the *CoEvolution Quarterly* and the *Whole Earth Review* as well as the original organizer of the Lake Tahoe Hacker's Conference. Among his books are *How Buildings Learn: What Happens After They're Built,* 1995, and *The Media Lab: Inventing the Future at MIT,* 1988.

3. Mr. John Peterson, President of the Arlington Institute and a noted futurist, devised the original two-dimensional matrix, war-peace, here-there to make the point that we train, equip, and organize our defense forces for "war, there" when in fact the bulk of the modern threat is "here, home." The author added the dimension of time to drive home the point that in this age of *ad hoc* coalitions and "off-the-shelf" nuclear and chemical take-out, we must be ready to deal with emergent threats on a "come as you are" basis.

4. See Robert D. Steele, "Information Peacekeeping: The Purest Form of War," immediately following the present paper; "Virtual Intelligence: Conflict Resolution and Conflict Avoidance Through Information Peacekeeping," *Proceedings* of the Virtual Diplomacy Conference, April 1-2, 1997, in Washington, DC, U.S. Institute of Peace;

"Intelligence and Counterintelligence: Proposed Program for the 21st Century," OSS White Paper, April 14, 1997; "The Military Perspective on Information Warfare: Apocalypse Now," *Enjeux Atlantiques,* No. 14, February 1997; "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information," *Government Information Quarterly,* Summer 1996; "Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare," in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, contributing eds., *Cyberwar: Security, Strategy, and Conflict in the Information Age,* AFCEA, 1996; "The Military Perspective on Information Warfare: Apocalypse Now," Speech*, Proceedings of the Second International Conference on Information Warfare*, January 19, 1995; "Reinventing Intelligence: The Vision and the Strategy," *International Defense and Technologies*, December 1995; "Hackers as a National Resource," Presentation, Hackers on Planet Earth, New York, August 13-14, 1994; and "War and Peace in the Age of Information," Lecture, Naval Postgraduate School, August 17, 1993.

5. Observation made on the C4I List by Perillo@DOCKMASTER.NCSC.MIL, together with a number of other quotations from documented sources, some cited elsewhere in this paper.

6. Winn Schwartau, personal communication, March 17, 1998.

7. The author and Winn Schwartau, author of *Information Warfare: Chaos on the Electronic Superhighway*, Thunders Mouth Press, 1994, between them know most of the major hackers as well as most of the major straight electronic security gurus. In this one instance, what emerged as remarkable was who was not consulted, in most cases because the NIE did not provide for discovery of expertise and interviewing of experts outside the beltway. Unfortunately, the same was true for the PCCIP.

8. The Surface Water and Related Land Resources Development Map is designed to portray both the development and preservation aspects of Federal water resources activities, the main theme being the spatial distribution of dams and reservoirs. Dams are shown that have normal storage capacity of at least 5,000 acre-feet, or a maximum storage capacity of at least 25,000 acre-feet. This includes about 800 dams owned by Federal agencies and about 2,000 dams owned by non-Federal organizations. *FGDC Manual of Federal Geographic Data Products - Surface Water Map* can be found at www.fgdc.gov/FGDP/Surface_Water_Map.html.

9. He made this comment in his remarks to an audience of 629 intelligence professionals attending the first open source intelligence

conference, "National Security and National Competitiveness: Open Source Solutions," December 2, 1992, in Washington, DC.

10. During the major floods of 1993, four of the six bridges were closed. Major rail traffic delays and costs were incurred as traffic was routed to the northern and southern bridges still in operation. "Flooding Halts Railroad Traffic Through Major East-West Hub: Freight Lines, Amtrak Rust to Find Detours in North and South," *The Washington Post*, July 27, 1993, p. A4.

11. The first "top ten" listing to be seen by the author was created by Peter Black. His article, "Soft Kill: Fighting infrastructure wars in the 21st century," *WIRED Magazine*, July/August 1993, listed the following targets:

- Culpepper Switch, handling all electronic transfers of federal funds;
- Alaska Pipeline, carrying ten percent of the domestic oil;
- Electronic Switching System, ESS, managing all telephony;
- Internet, the communications backbone of science and industry;
- Time Distribution System, upon which all networked computers depend;
- Panama Canal, major choke point for U.S. trade;
- Worldwide Military Command and Control System (WWMCCS);
- Big Blue Cube, Pacific clearinghouse for satellite reconnaissance;
- Malaccan Straits, Singapore, the maritime link between Europe-Arabia and the Pacific;
- National Photographic Interpretation Center, processing center for imagery.

12. Winn Schwartau, personal communication, March 17, 1998.

13. *Ibid*. See also note 1.

14. In 1992 a major U.S. intelligence community entity, one extremely familiar with computers, briefed the Information Handling

Committee on the results of its 1-year survey of viruses arriving at its loading docks in shrink-wrapped products. The total number found was 500.

15. The author, Speech, Hackers on Planet Earth. Hackers, as the author has noted with frequency, are *not* the problem, not even the symptom of the problem—they are a national resource in that they are demonstrating, without causing significant damage, just how vulnerable all of our systems are.

16. Mich E. Kabay, *The NCSA Guide to Enterprise Security: Protecting Information Assets*, New York: McGraw-Hill, 1996. Fig. 1, p. 11. The figure in the book is superseded by the present table, provided by Dr. Kabay in personal communication, March 12, 1998.

17. A typical assessment of this looming access problem is found in *CIWARS*, Vol. 10, Issue, Intelligence Report, November 2, 1997. <www.iwar.org> contains this and many other interesting reports on electronic vulnerabilities around the world.

18. Note 6.

19. At the time the author surveyed several experts, including Professor William Caelli in Australia, and one of the top computer security advisors to the National Security Agency.

20. In May 1997 an Information Security Industry Survey done by Delotte and Touche LLP, with 1225 organizations surveyed, reported that 40 percent blamed "unclear responsibilities" and 26-30 percent blamed "lack of central authority" as the reasons why they could not come to grips with computer and telecommunications security requirements. As noted in February 11, 1998, email from <Peerillo@*DOCKMASTER.NCSC.MIL*>.

21. Statement made at OSS '96, where Mr. Stratton, a computer security engineer, was a speaker, together with his partner, Mr. Chris Goggans.

22. The author coined the term in 1994. For two papers defining this aspect, see note 4.

23. In 1995 the author proposed the following annual budget for national information security:

1. Enact a National Information Strategy Act	$20,000.000
2. Establish a National Center for Electronic Security	40,000,000
3. Declassify and Promulgate the Threat	10,000,000
4. Establish C4 Security as a Fiduciary Responsibility (in Private Sector)	30,000,000
5. Establish Basic and Advanced C4 Trusted System Standards	100,000,000
6. Authorized and Encouraged Public Keys and Privacy Measures	200,000,000
7. Establish a National Information Foundation	25,000,000
8. Establish a C4 Security Testing and Certification Program	200,000,000
9. Establish an Electronic Security and Counterintelligence Division (in FBI)	25,000,000
10. Establish a Joint Information Warfare Corps and Center	50,000,000
11. Reorient Military C4 Toward Open Systems	100,000,000
12. Establish a Joint Military IW Research Consortium (with Private Sector)	100,000,000
13. Influence Civilian Information Technology Research (re embedded security)	100,000,000

See concluding section of speech in Montreal, note 4. In 1997 the author proposed a $1.6 billion-a-year budget for the national virtual intelligence community, comprised of $250 million for commercial imagery to meet DoD and USG needs; $250 million to meet NATO/Partner for Peace open source intelligence needs; $250 million for U.S. Intelligence Community access to open sources; $50 million for a University of the Republic to bring leaders from various sectors together; and $400 million for two related largely classified initiatives. Detailed in "Intelligence and Counterintelligence: Proposed Program for the 21st Century," OSS White Paper, April 14, 1997, at http://www.oss.net/oss21>.

INFORMATION PEACKEEPING: THE PUREST FORM OF WAR*

Robert D. Steele

Information Peacekeeping is one of two neglected aspects of Information Operations, a new concept that up to this point has focused almost exclusively on Information Warfare, and avoided dealing with the substance of All-Source Intelligence, or the proactive possibilities of Information Peacekeeping. Information Peacekeeping is the active exploitation of information and information technology so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority, are open source intelligence; information technology; and electronic security and counterintelligence. Information Peacekeeping is the strategic deterrent as well as the tactical force of first resort for the 21st century. Virtual Intelligence, a supporting concept, is the foundation for informed policy-making, judicious acquisition management, effective contingency planning and execution, and timely public consensus-building. By its nature, Information Peacekeeping must rely almost exclusively on open sources and services available from the private sector; this requires the crafting of a new doctrine of national intelligence that places the critical classified contributions of the traditional national intelligence communities within the context of a larger global information community. Information Peacekeeping is the purest form of war, but most traditional warriors will be reluctant to accept its most fundamental premise: that intelligence is indeed a virtual substitute for violence, for capital, for labor, for time, and for space. Information Peacekeeping is in effect both a strategy for government operations and a national security strategy with global

* In Alan Campen and Douglas Dearth, *CYBERWAR 2.0: Myths, Mysteries, and Realities*, AFCEA Press, June 1998, pp. 277-293.

reach; consequently it has profound implications for how we train, equip, and organize our government and our military.

Introduction: Intelligence as Munition.

Time and time again, the U.S. defense and intelligence communities rush to spend billions on technology, while routinely ignoring the challenges and opportunities inherent in human collection, open-source collection, foreign area expertise, and human all-source analysis.[1] We do it in mobility systems, in weapons systems, in command-and-control systems and in intelligence systems. Sadly, leaders in all corners of the Department of Defense (DoD), at all levels, continue to abdicate their responsibility for *thinking* at the strategic, operational, tactical and technical levels, and have surrendered their forces to the mindless flow of self-generated bits and bytes.[2]

A majority of the U.S. military leadership still does not "get it." The Revolution in Military Affairs is a joke. It is nothing more than lip service, substituting astronomically expensive systems with no sensor-to-shooter guidance nor any relevance to three of the four warrior classes, for outrageously expensive systems with no sensor-to-shooter guidance and dated relevance to one of the four warrior classes. The three warrior classes we must confront in this new era are: the low-tech brutes (transnational criminals, narco-traffickers, terrorists); the low-tech seers (ideological, religious, and ethnic groups unable to accept conventional relations among nations); and high-tech seers (a combination of information terrorists or vandals, and practitioners of economic espionage).[3] Most of our training, equipment, and operational doctrine are completely unsuited to meeting the threat from these three warrior classes. Perhaps even more disturbing is the fact that our national "order of battle" must now fully integrate our government civilian agencies and our private sector information reserves, but we have no one in a leadership

position who is willing or able to deal with this harsh and urgent reality.

The real revolution is being led by a few original thinkers who have yet to be heard on Capitol Hill and whose thoughts are a decade from effecting fruitful changes in how we train, equip, and organize our nation for war. Alvin and Heidi Toffler were among the first to articulate the fact that information is a substitute for wealth and violence, for capital, labor, time, and space.[4] Pilots and ship drivers may never forgive Martin Libicki for reframing their platforms as delivery vehicles for intelligence-driven operations.[5] Winn Schwartau overcame his Hollywood and rock-and-roll past ultimately to inspire a Presidential Commission on Critical Infrastructure Protection.[6] Colonel James Clark blew past the naysayers, with support from the Vice Chief of Staff of the Air Force to bring EAGLE VISION in as an operationally effective means of putting real-time commercial imagery into tactical service—something the National Reconnaissance Office (NRO) and the National Imagery and Mapping Agency (NIMA) refused to contemplate and still resist at every level.[7]

Information Peacekeeping,[8] the subject of this paper, is the purest form of war. It shapes the battlefield, it shapes the belligerents, and it shapes the bystanders in such a way as to defeat the enemy without battle—in such a way as to achieve U.S. policy objectives without confrontation and without bloodshed. Sun Tzu would approve.[9]

At the strategic level Information Operations (Figure 7) must be seen as a triangle in which all-source intelligence, information warfare, and information peacekeeping are seamlessly integrated and inherent in all aspects of military and civilian operations. *Perhaps the most important aspect of information operations in the 21st century is that it is not inherently military; instead, civilian practitioners must acquire a military understanding and military discipline in the practice of information operations, if they are to be effective.*

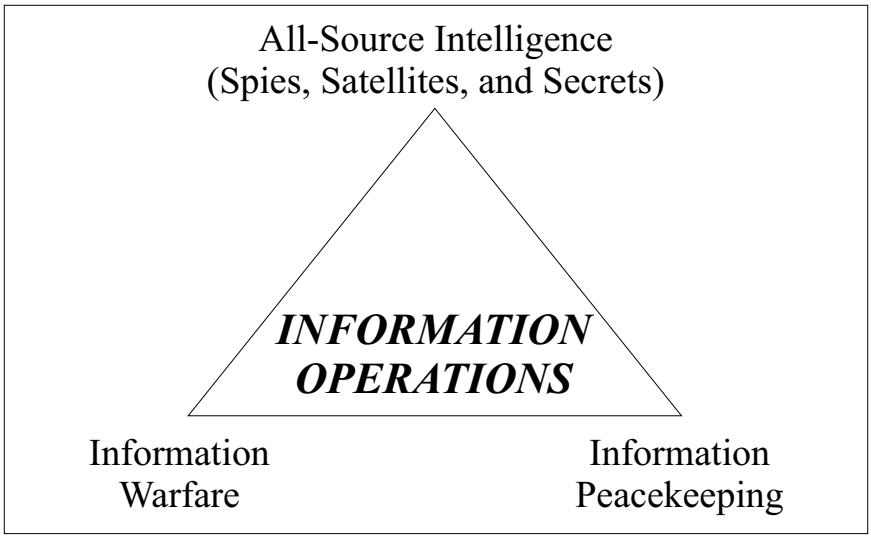

Figure 7. Strategic View of Information Operations.

Information Operations tend to be viewed as a strategic form of Information Warfare, but this is a much too narrow view which deprives the policymaker, acquisition manager, and commander of two-thirds of the "firepower" represented by a more accurate and well-rounded understanding of Information Operations.

All-Source Intelligence is the critical classified element of Information Operations which assures all parties being supported that they are receiving essential indications and warning intelligence, current intelligence, and estimative intelligence, to name just a few kinds of all-source intelligence.

Information Peacekeeping is the active exploitation of information and information technology so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority, are: open-source intelligence; information technology; and electronic security and counterintelligence.

Information Peacekeeping is a *strategic deterrent* that radically increases the ability of the practicing nation to avoid or resolve conflict in relation to all four warrior classes

and across the complete spectrum of government operations—not only military but diplomatic, commercial, agricultural, etc.

All three aspects of Information Operations—the obvious one of Information Warfare and the two less obvious aspects of All-Source Intelligence and Information Peacekeeping—share one critical component: open-source intelligence (Figure 8). No aspect of Information Operations can be conducted effectively without full access to a cooperative private sector that controls the vast majority of national knowledge resources—the "information commons."[10] Once thought of in this light, it becomes evident that the center-of-gravity for Information Operations is in the civil sector—the private sector.

Interestingly, this perspective also makes it clear that the importance as well as the presence of secrecy declines dramatically as one moves from the left "warfare" side of the equation to the right "peacekeeping" side of the equation. In fact, fully 80 percent of the intelligence "solution" comes

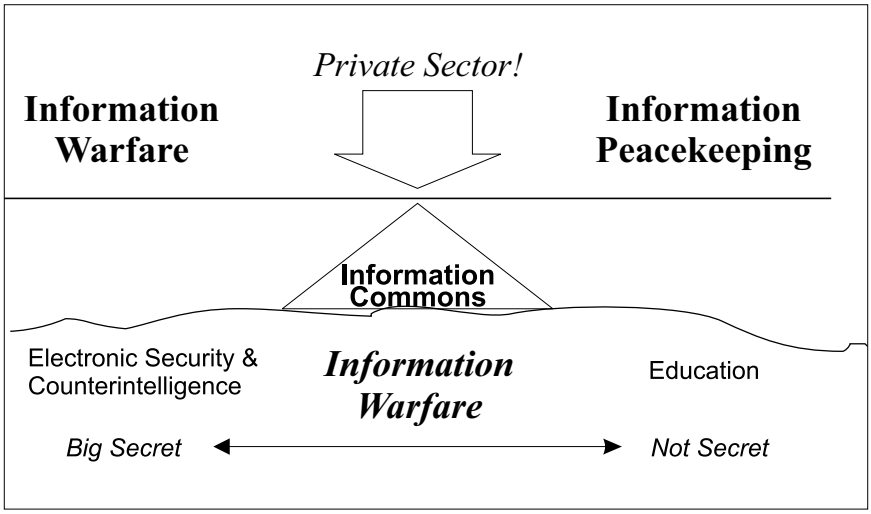

Figure 8. The Center of Gravity for Information Operations.

from open rather than classified sources, and it is incumbent on the consumers of intelligence—not the producers—to harness these *open* sources.[11]

Consumer Communities: Getting Back to Basics.

For those tempted to question the substantial depreciation in the value of secrecy, a glimpse into the cognitive battlefield—the mind of a typical consumer—is instructive (Figure 9). The four consumer communities—the policymakers, the acquisition managers; the commanders and their staffs; and the public—each require tailored intelligence which is largely unclassified in nature, collected and delivered in very short time-cycles, and often most valued when it is least cumbersome (i.e., concise and to the point). The public must be treated as a real-time partner to decision making in foreign and defense policy. The policymaker needs, and must use, tailored open-source intelligence products to ensure that the public is informed

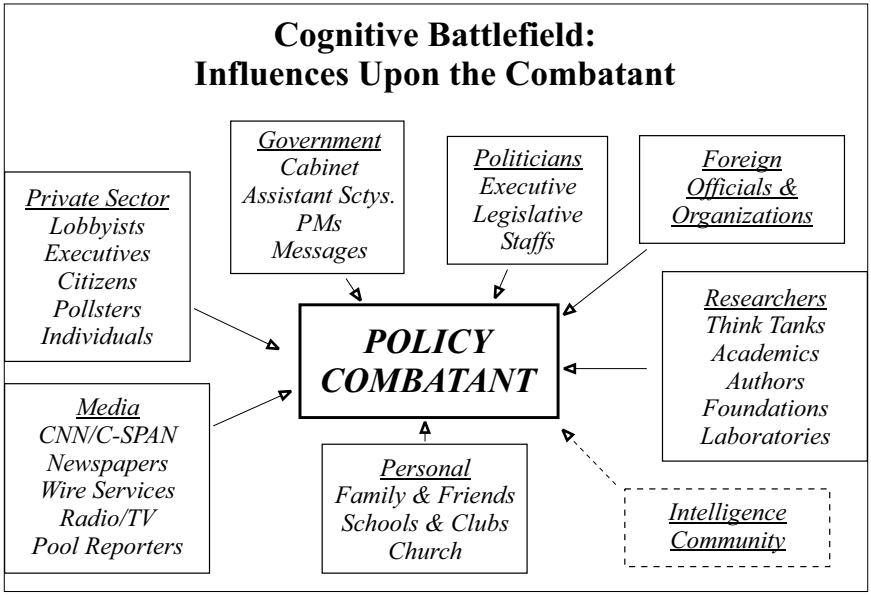

Figure 9. Understanding the Cognitive Battlefield.[12]

enough about a situation to support administration decisions both during and after the fact.

This boils down to two major facts in the world of Information Operations:

1. Ninety percent of the information reaching a typical consumer—at whatever level—is unclassified and unanalyzed; and

2. Neither the consumer nor the producer of intelligence has yet developed a capability for discovering, discriminating, distilling, and digesting *intelligence* within this overwhelming information environment replete with multiple sources of conflicting information.

Perhaps the most important aspect of Information Operations is the defensive aspect. Our highest priority, one we must undertake before attempting to influence others, is that of putting our own information commons in order. We must be able to assist and support our consumers with knowledge management concepts, doctrine, and capabilities, such that they can "make sense" of the information chaos surrounding them. This is perhaps most vital within the policy-making community.

Accepting the larger definition of Information Operations proposed in this paper, there are distinct benefits for each major constituency group:

- **Policymakers** will have significantly improved intelligence that fully appreciates cultural, economic and regional nuances not well covered by classified sources, and will have open-source intelligence products that can be readily shared with both home and host-country counterparts, press, and public.

- **Acquisition Managers** will be able to obtain strategic generalizations that accurately evaluate the threat in their respective mission areas at each level of analysis, while also establishing regional generalizations upon which to make sounder

decisions about logistics and C4I supportability as well as countermeasure requirements.

- **Commanders and Staffs** will have access to unclassified open-source intelligence, including commercial imagery, that are essential to begin the contingency planning process, to execute humanitarian assistance operations, to guide classified collection management, and to place classified reporting in context. Open source intelligence will provide cover for communicating critical battlefield information to coalition and civilian partners including non-governmental organizations, and in general will provide for the common view of the battlefield or issue area essential to complex command and control. As will be noted in the section on global geospatial shortfalls, for this constituency group the most vital benefit is the ability of commercial imagery to address the 90% of the requirements for image maps that have not been met and will never be met by classified sources.

- **Publics** will have access to relatively straightforward and reliable explanations of foreign and domestic conditions and perceptions that are causing policymakers to take action, or requiring the acquisition of certain capabilities, or requiring the preparation of forces for employment. In the world of global information, the first three constituencies cannot rely on the media to do an accurate job of reporting; the public must receive a level of "intelligence support" which heretofore has not been necessary but which is now vital to the smooth transition from peace to war, or vital to reasonable popular understanding of particular crisis response options.

Net Assessments: An Operational View of Knowledge.

The acquisition community has a different sort of problem: the absence of an effective model for providing sophisticated threat assessments in relation to both the levels of analysis and the real-world conditions under which the systems are to be used.

Absent such a model, our intelligence analysts have no alternative but to continue doing what they do today: concluding that every threat is a "worst case" threat to be evaluated strictly on the basis of its maximum technical lethality, while avoiding coming to grips with generalizations about the environment which should, but do not, influence acquisition decisions.[13]

In fact, the threat changes in relation to both the level of analysis and the geographic-civil context within which friendly and enemy military capabilities are deployed (Figure 10). We will focus only on the first aspect here. Taking Libyan tanks in 1990 as an example:

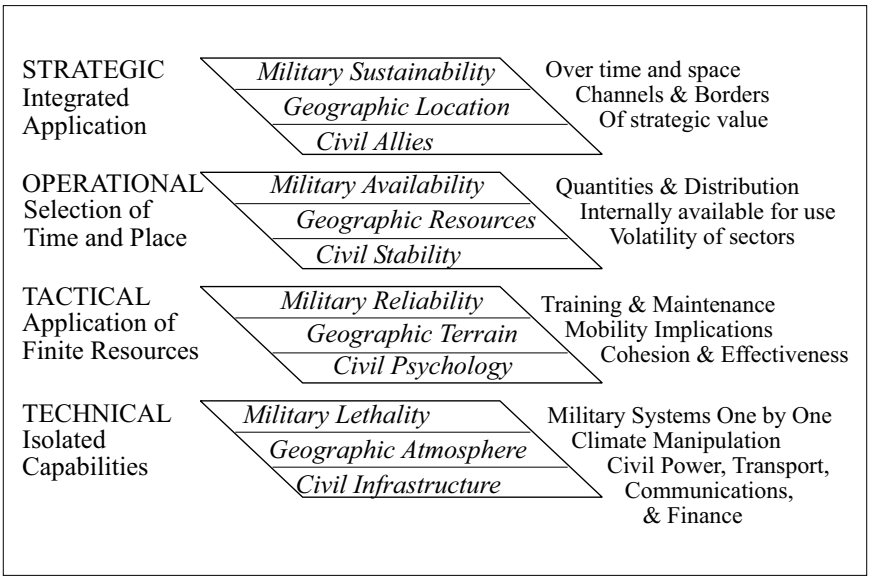

Figure 10. Net Assessment and Open Source Intelligence.

- At the technical level (lethality), since they are the best tanks that Soviet money can buy (at the time, the T-72), they must be evaluated as a very high threat. *This is where existing practices start and stop.*

- At the tactical level (reliability), once one appreciates the lack of training for the crews, the long-term storage of many of the tanks in the open, and the cannibalization of some tanks to keep others operational, the threat drops to low.

- At the operational level (availability), given the number of tanks scattered around, the threat rises to medium.

- At the strategic level (sustainability), the threat drops again to low for obvious reasons associated with both command and control and logistics supportability deficiencies.

The United States cannot pretend to have a viable Information Operations doctrine so long as this travesty of analytical impoverishment is allowed to continue. There is not a single intelligence report in existence today (nor available from the past) which reflects this level of sophistication and distinction, and that is something that must change soon. We continue to design and acquire systems in isolation from the real-world threat and the real-world environment in which they are to be employed. This robs the nation of scarce resources which could be applied much more effectively in other pursuits, including the pursuit of Information Peacekeeping Operations.

There is one other major deficiency in U.S. intelligence doctrine: its rather naïve focus on just three major areas of interest: the traditional two areas of political-military intelligence and scientific and technical intelligence; and the more recently activated area of economic intelligence. Despite the good efforts of some leaders in the past, notably Secretary of State Warren Christopher,[14] the United States

continues to give short shrift to the critical intelligence challenges associated with sociological and ideo-cultural intelligence; demographic intelligence; and environmental intelligence. In order to plan and execute Information Operations that are precise and likely to have the desired outcome, the United States must radically expand its concepts and doctrine for national intelligence so as to be able to comprehend the full range of intelligence challenges across both domains of interest and nations of interest. It cannot do this if it relies primarily on the classified intelligence community and secret sources.

Information Peacekeeping: The Heart of Information Operations.

Information Peacekeeping is the active exploitation of information and information technology—in order to modify peacefully the balance of power between specific individuals and groups—so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority, are: open-source intelligence (providing useful actionable unclassified information); information technology (providing "tools for truth" that afford the recipient access to international information and the ability to communicate with others); and electronic security and counter-intelligence (a strictly defensive aspect of Information Operations). (See Figure 11.)

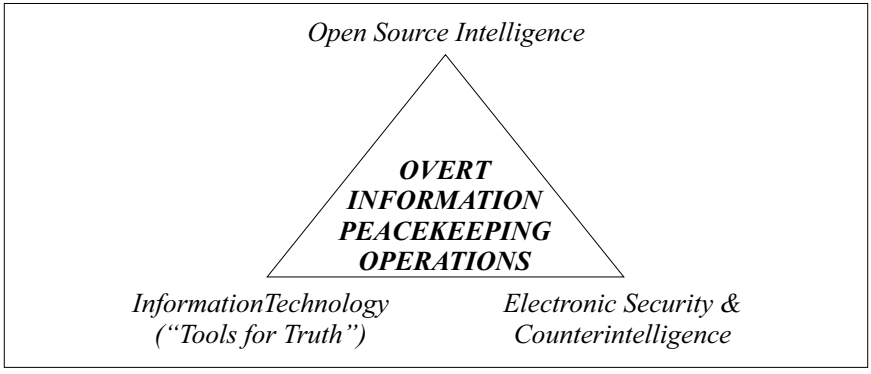

Figure 11. Elements of Overt Information Peacekeeping Operations.

To understand what this means, it is useful to specify what Information Peacekeeping is *not*. Information Peacekeeping is not:

- Application of information or information technology in support of conventional military peacekeeping operations, or in support of United Nations, coalition, or diplomatic operations.

- Development and execution of traditional psychological operations or deception operations that strive to manipulate perceptions in order to achieve surprise, or to cause actions to be taken that would not have been taken if the true circumstances were known.

- Covert action media placement operations, covert action agent of influence operations, or covert action paramilitary operations

- Clandestine human intelligence operations or overt research operations.

Although Information Peacekeeping is not to be confused with clandestine or covert methods, there are gray areas. Information Peacekeeping may require the clandestine delivery of classified or open source intelligence, or the covert delivery of "tools for truth" such as the traditional radio broadcast equipment, or the more recently popular cellular telephones and facsimile machines. Information Peacekeeping may also require covert assistance in establishing and practicing electronic security and counterintelligence in the face of host country censorship or interference.

On balance, then, Information Peacekeeping is by its nature most powerful and effective when it relies exclusively on open sources of information, the delivery of open-source intelligence, and on overt action. Under these conditions, it is incontestably legal and ethical under all

applicable rules of law, including host country and non-Western cultural and religious rules of law and custom.

Information Peacekeeping is the tactical "force of first resort" for 21st century operations, and every theater and every major command, must have an order of battle able to conduct overt Information Peacekeeping Operations in all three of its major aspects.

Existing staff functions are not adequate to this challenge at this time. Taking each of the major staff elements for a theater command in turn:

- J-1 (Administrative). Generally includes handling of refugees and prisoners of war. No concepts, doctrine, or "order-of-battle" for treating information as either a munition or a critical logistics elements. Of most immediate concern: no J-1 (or G-1 or S-1) appears to have at hand an approved Table of Organization and/or Table of Equipment for handling humans who are placed under military care in a tactical environment.

- J-2 (Intelligence). Generally reactive and apathetic—takes whatever it can get from classified national intelligence systems. Does not have the concepts, doctrine, funding, security permissions, or "order-of-battle" for going out and getting open-source intelligence with which to provide direct support to theater operations.

- J-3 (Operations). Focuses strictly on placing munitions on target, positioning troops, and planning movements. Does not have concepts, doctrine, or an "order-of-battle" with which to use information as a substitute for munitions or men. Note that the execution of Information Warfare attacks, or the conduct of Psychological Operations, do not count and do not have the same effect as Information Peacekeeping Operations.

- J-4 (Logistics). Focuses on beans, bullets, and band-aids. Not responsible for evaluating or considering how full or empty the various constituencies are with respect to information essential to their mission. Imagine how effective a command might be if its information requirements—and those of its coalition partners and civilian agency counterparts—were treated with the same seriousness as fuel stocks or critical spare parts for fighter aircraft.

- J-5 (Plans/Other). Focuses on plans in isolation. Is not held accountable for declaring specific plans to be unsupportable due to a lack of intelligence or maps. The fact is that most theater contingency plans have made no provision for acquiring the necessary open-source intelligence—including commercial imagery—because everyone is assuming that national capabilities will suffice and will be made available. This is fiction.[15]

- J-6 (Communications). Focuses on administration of limited bandwidth and assignment of limited communications and computing resources, as well as subsequent oversight of the entire architecture. Is not held accountable for considering how the theater will communicate with coalition and civilian partners who are not equipped to U.S. standards. Is burdened by a vast and very expensive C4I architecture designed by the military services, all of whom assumed that the United States would always be fighting a unilateral military action in which all parties have the necessary clearances to be part of the largely classified theater command- and-control system. In particular, the J-6 is not held accountable for ensuring that externally acquired data, including maps, and external nodes, including non-governmental groups, can be fully integrated into the larger Information Operations environment within which the CINC must operate.

Others can focus on the information technology and electronic security aspects of Information Peacekeeping—this article will conclude with an examination of the most important aspect of Information Peacekeeping: the use of open source intelligence to understand, shape, and dominate the knowledge terrain in the "battle area."

Virtual Intelligence: The Brain of Information Operations.

In the words of Richard Kerr, speaking in late 1997: "The Intelligence Community has to get used to the fact that it no longer controls most of the information."[16] What this really means is that the United States can no longer rely exclusively on classified sources for the bulk of its intelligence, nor can the intelligence consumer communities—including the very important military operational and tactical consumers—assume that all of its intelligence needs will be met by the U.S. Intelligence Community as it has traditionally operated.

The Commission on Intelligence, a bi-partisan endeavor that included members appointed by both parties of the House and Senate, as well as members appointed by the Administration, offered two pertinent recommendations:[17]

- The U.S. Intelligence Community is "severely deficient" in its access to open sources, and this should be a "top priority" both for the attention of the Director of Central Intelligence and for funding.

- The consumers of intelligence should not refer requirements to the U.S. Intelligence Community when they can be answered predominantly through open sources, but rather should create their own open source intelligence.

- The Commission on Intelligence made these two recommendations because its investigations clearly documented that in the Information Age, the vast

majority of usable, relevant information necessary to support policymakers, acquisition managers, and commanders is available in unclassified form from private sector sources—open sources are by definition sources which are legally and ethically available to anyone.[18]

The greatest obstacle to improved use of open sources is not that of *access*, which is freely or inexpensively available to all, but rather that of *acceptance*. The two most erroneous perceptions among experienced professionals who should know better are that open sources are "merely a collection of newspaper clippings" (in the words of a senior Intelligence Community official) or "the Internet" (in the words of a general officer). Figure 12 shows an illustrative, but by no means comprehensive, range of open sources, software, and services.

SOURCES	SOFTWARE	SERVICES
Current Awareness (e.g. Individual Inc.)	Internet Tools (e.g. NetOwl, Web Compass)	Online Search & Retrieval (e.g. NERAC, Burwell Enterprises)
Current Contents (e.g. ISI CC Online)	Data Entry Tools (e.g. Vista, BBN, SRA)	Media Monitoring (e.g. FBIS via NTIS, BBC)
Directories of Experts (e.g. Gale Research, TEL TECH)	Data Retrieval Tools (e.g. RetrievalWare, Calspan)	Document Retrieval (e.g. ISI Genuine Document)
Conference Proceedings (e.g. British Library, CISTI)	Automated Abstracting (e.g. NetOw., DR-LINK)	Human Abstracting (e.g. NFAIS Members)
Commercial Online Sources (e.g. LN, DIALOG, STN, ORBIT)	Automated Translation (e.g. SYSTRAN, SRA NTIS-JV)	Telephone Surveys (e.g. Risa Sacks Associates)
Risk Assessment Reports (e.g. Forecast, Political Risk)	Data Mining & Visualization (e.g. Visible Decisions, TASC Textor)	Private Investigations (e.g. Cognos, Pinkertons, Parvus)
Maps & Charts (e.g. East View Publications)	Desktop Publishing & Communications Tools	Market Research (e.g. SIS, Fuld, Kirk Tyson)
Commerical Imagery (e.g. SPOT, Radarsat, Autometric)	Electronic Security Tools (e.g. SSI, PGP, IBM Crytolopes)	Strategic Forecasting (e.g. Oxford Analytics)

Figure 12. Illustrative Range of Open Source Niches.

Also to be noted is the distinction between those resources which are readily available within the U.S. Intelligence Community; within the rest of the government; within the nation (i.e., in the private sector with its

universities, information brokers, businesses, media, and other information activities); and within the larger global information community. It is absolutely essential that each intelligence producer and consumer have a "map" of this larger knowledge terrain, and a strategy for assuring their ability to discover, discriminate, distill, and digest critical open-source information and intelligence.

Those familiar with the existing security and procurement practices of both the U.S. Intelligence Community and the military operations environment will recognize that there are enormous obstacles to progress in this area. An ignorance of what is available in the private sector and a reluctance to reveal our rather obvious interests cause many to eschew the benefits of open-source intelligence. Simultaneously, our procurement system is biased in favor of multi-million dollar contracts with beltway bandits whose expertise is largely in how to win procurements that focus predominantly on providing technology solutions, rather than the direct ability to harness world-class expertise. We must move rapidly toward a more open intelligence environment in which individual analysts and individual desk officers are empowered with the knowledge and the procurement authority to obtain "just enough, just in time" open source information and intelligence support.[19]

Geospatial Gaps: The Achilles' Heel of Information Operations.

In the over-all scheme of information operations, there is no greater debility than the almost total lack of global geospatial mapping data at a scale of 1:50,000.

- This is the level necessary for tactical movement of troops under fire, for the coordination of combined-arms support, for the targeting of precision munitions, and for the simulation of three-dimensional nape-of-the-earth approaches for sensitive aviation missions.

- It is also the level at which automated all-source data fusion (the Holy Grail for all intelligence technocrats) and automated multi-source data visualization become "real."

The National Imagery and Mapping Agency (NIMA) acknowledges that it has less than 10% of the world at this level, and has no plans for acquiring commercial imagery in order to create a global geospatial database at this level.[20] As the Defense Mapping Agency (DMA) discovered during the Gulf War, NIMA is also incapable of creating 1:50,000 maps—even with full support from commercial imagery sources—in less than 60-90 days.[21]

The broad nature of the deficiency can be defined as follows:

- For Africa, where many of our unexpected contingencies occur, we do not have acceptable mapping data for 13 countries including Ethiopia, South Africa, and Uganda.

- For Asia and the Pacific, an area many consider central to our economic future and also highly subject to regional disturbances, we do not have acceptable mapping data for 12 countries, including China, Indonesia, and Papua New Guinea, nor for the four major island groups including the contested Spratly Islands.

- For Europe and the Mediterranean, Greece and Turkey remain completely uncovered, despite their importance to NATO, their traditional rivalry, and the role of Turkey in relation to the former Soviet Republics, Iraq, and Iran.

- For the Western Hemisphere, our own "back yard," we lack acceptable mapping data for 13 countries, including Argentina, Colombia, Mexico, and Paraguay.

This deficiency will continue to exist for the next decade or two—and beyond—unless there is a deliberate decision made at the Presidential level, with full support from the Joint Chiefs of Staff, to resolve this deficiency immediately. The cost for resolving it has been estimated by knowledgeable senior leaders of NIMA at between $250 million and $500 million a year in commercial imagery procurement for the next five to six years.[22] This cost would cover, among other important projects, complete 1:50,000 coverage of China, the Amazon, and Africa. In combination with the planned shuttle mission in 2002 to collect precision points (Digital Terrain Elevation Data) for the entire Earth, this will allow the United States to have a phenomenal intelligence and Information Operations advantage, as the only country in the world with a complete accurate map of every significant portion of the Earth at the 1:50,000 scale.

In the absence of such geospatial data at the 1:50,000 level, policy options are severely constrained. Precision munitions cannot be used until the imagery and mapping data are collected and processed; Special Operations units and drug interdiction teams are at a major disadvantage; conventional military and law enforcement operations cannot be properly planned and executed; humanitarian assistance and other coalition operations are handicapped—the list goes on and on.

There is no one today, at any level of the military and certainly not within the White House or any other Cabinet department, who is willing and able to make this case before the Secretary of Defense and the President of the United States—hence we continue to plan for the future with our "eyes wide shut."[23.]

Conclusion: New Doctrine for a New Era.

Information Peacekeeping is in effect both a strategy for government operations and a national security strategy with global reach; consequently it has profound implications for

how we train, equip, and organize our government and our military (Figure 13).

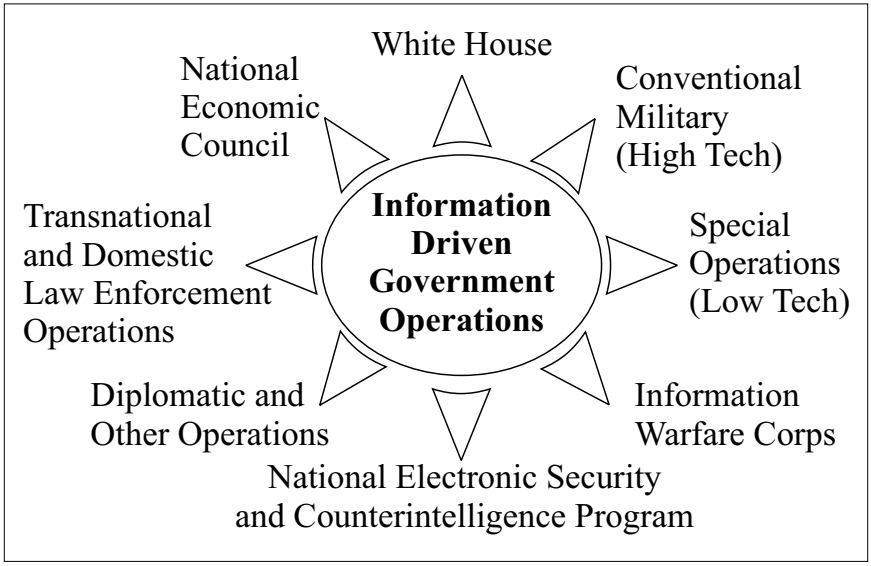

Figure 13. New Government Operations Doctrine.

In the final analysis, we must come to grips with the fact that our government today is an industrial-era government, woefully inadequate in all respects as to the management of internal information and the acquisition and exploitation of external information. This in turn renders us wastefully ineffective in the planning and execution of global influence operations, both those that use information and those that use violence or other means.[24]

We can, however, remedy this situation. The following steps are recommended:

1. Provide the Director of Central Intelligence with the centralized program management authority over all classified collection and production programs, as envisioned in the National Security Act of 1992 (which was not adopted by Congress).[25]

2. Create a new Director of National Intelligence within the existing National Security Council (NSC) structure,

responsible for oversight of government information operations from a substantive point of view.

a. Elevate the National Intelligence Council by moving it to this new office, and expand it modestly by creating National Intelligence Officers corresponding to each of the major consumer groups in government and in the private sector. The existing geo-functional NIO's would become Associate NIOs and would continue to serve as the focal points for regional and topical intelligence management.

b. Provide $1 billion a year for a Global Knowledge Foundation, modeled after the National Science Foundation, but responsible for nurturing (but not regulating or overseeing) distributed centers of expertise world-wide, all of which can comprise the "Virtual Intelligence Community," or, in traditional terms, a truly *national* intelligence reserve.

c. Subordinate both classified intelligence and Departmental intelligence endeavors to a larger national intelligence community that uses open sources of intelligence as the source of first resort,[26] while restoring the classified intelligence community to its rightful place as the source of *last resort*, authorized to use whatever means necessary to acquire critical information *not available through other means*. Fence the existing classified budgets for a decade, specifically precluding the Secretary of Defense from reducing those portions of the intelligence budget concealed within Department of Defense budget lines.

d. Subordinate the existing Electronic Security and Counter-intelligence Program, for which funding on the order of $1 billion a year has been recommended by the President's Commission on Critical Infrastructure Protection, to this larger office, but leave executive authority for its execution with the Federal Bureau of Investigation. This is essential, because the "Virtual Intelligence Community" cannot exist without national

electronic security and counter-intelligence guarantees to the private sector.

Among the first steps a new Director of National Intelligence might take would be:

1. Establish a National Net Assessments Center to apply net assessment methods to domestic issues as well as non-military international issues. The existing military Net Assessments Office could, with some significant changes in focus and the integration of representatives from the other Departments of government, serve as the cadre for this broader national center.

2. Establish a National Open-Source Consortium to transfer knowledge of open sources, software, and services to all levels of government, as well as all elements of the private sector.

3. Establish four small Threat Assessment Centers corresponding to each of the four warrior classes, and modeled after the DCI Centers now in existence for terrorism and "crime and narcotics," but with a major emphasis on the collection and exploitation of open sources. Alternatively, these could be small five-person oversight cells within the office of the DNI/NSC.

4. Establish a commercial imagery fund able to procure, at substantial discounts, all commercial imagery needed by the civilian departments, the military, law enforcement, and the NATO/Partners for Peace program.[27] Rather than entrust NIMA with these funds (NIMA may not be around in the near future), the funds would be maintained by the DNI and allocated to the CINCs and Departments for expenditure as they each deem appropriate.

5. Establish a Presidential Commission on National Intelligence to examine how best to create an integrated information "order-of-battle" which fully harnesses the knowledge and information management skills of both the federal and state governments, and the private sector. The Commission would have as a specific objective defining a

new national intelligence reserve concept that facilitates the inclusion of civilian experts (including international experts), on an "as needed" basis.

Finally, then, we come to "who cares?" and "why should we?" What do we gain? We gain a swift, smart, sleek government able to provide for a "360°" or—in more modern terms—a "spherical"[28] defense at home and abroad, with revolutionary improvements in both our ability to influence others, and our ability to spend money wisely—fewer "hangar queens" and more "just right" stilettos. If we do not do this, if we continue to muddle through, then low-tech brutes will continue to slip through our crude defenses, low-tech seers will continue to be invisible to our warning networks, and high-tech seers will spend the next 20 years freely practicing information terrorism and vandalism, or plundering our electronic intellectual property and digital storehouses of wealth.

Only DoD has the mix of talent, resources, and influence to make the necessary things happen, and only DoD has the budget flexibility to permit realignment of the needed funds. It is *not* only DoD that must defend our nation from all enemies, domestic and foreign—this responsibility must fall evenly on every element of the government, including state and local governments. It *is*, however, DoD that must first rise to the challenge and lead us to a thinking about, and funding, a future where Information Peacekeeping is recognized as the purest form of war, and the only path to sustained peace and prosperity.

ENDNOTES

1. Overemphasis on expensive and narrowly focused technical collection has been a consistent concern in every major review of the U.S. Intelligence Community since technical solutions came into vogue in the 1960's. For a fine summary of the "Seven Sins of Strategic Intelligence" identified by the Church Commission in 1975, see the article by Dr. Loch Johnson, in *World Affairs*, Fall 1983. Dr. Johnson's many books, including his most recent, *Secret Agencies: U.S. Intelligence in a Hostile World*, Yale, 1996, stand as one of the more

balanced collections of commentary on this important topic. This theme is repeated in the two major reviews completed recently within the U.S. Government, the first in *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, March 1, 1996; the second in *IC21: Intelligence Community in the 21st Century*, Staff Study, House Permanent Select Committee on Intelligence, March 4, 1996. According to authoritative senior officers, we process less than 10 percent of what we collect on both the imagery and the signals sides of the technical collection function. Of the various major reviews conducted in the mid-1990s, *In From the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence*, 20th Century Fund Press, 1996, focuses most carefully on the urgent need for greater funding and quality control in all-source analysis. Mr. Mort Zuckerman and Mr. Richard Kerr were among the active contributors to this report. See also the background papers by Allan E. Goodman, Gregory F. Treverton, and Philip Zelikow.

2. In 1994 the author was invited by the National Research Council, affiliated with the National Science Foundation, to provide a review of the U.S. Army's multi-billion dollar multi-media communications plan for the future. The plan provided billions for internally-generated data, and nothing at all for acquiring the 80 percent of the information needed by the commander from external open sources, including commercial imagery. The plan also provided nothing for communicating with coalition partners, whose radios and typewriters remain incompatible with space-age communications and computing technologies.

3. The four warrior classes are discussed in detail in "The Transformation of War and the Future of the Corps," in *Intelligence Selected Readings—Book One*, U.S. Marine Corps Command and Staff College, AY 92-93.

4. See specifically Alvin Toffler, *PowerShift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, Bantam, 1990; and Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown, 1993.

5. One of the most intelligent and revolutionary writings pertinent to military doctrine is Martin J. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, National Defense University Press, 1994.

6. Schwartau's first book, *Terminal Compromise*, was considered by his lawyers to be so controversial that he was required to publish it as a novel. His follow-on, *Information Warfare: Chaos on the Electronic*

Superhighway, Thunders Mouth Press, 1994, set the stage for global discussion and is widely credited with awakening both the international press and the international military to this critical issue area.

7. EAGLE VISION/JOINT VISION is a ground station transportable in a single C-130 that is capable of taking real-time feeds from both SPOT IMAGE, 10 meter, satellites and national satellites. Today it can feed directly into aviation mission rehearsal systems and allow interactive three-dimensional fly-through practice. If the Army will pay attention and hook up its 18-wheeler topographic vans to one of these ground stations, it can produce 1:50,000 combat charts with contour lines on a "just enough, just in time" basis. As tactical capabilities to exploit commercial imagery expand, it will be increasingly difficult for NIMA and the NRO to justify their existing budgets and production costs.

8. The author coined this term in 1994 in discussion with Mr. James Q. Roberts, Director for Psychological Operations in the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Subsequently the author prepared the paper "Information Peacekeeping: Innovative Policy Options," for the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, presented at OSS '96, September 18, 1996.

9. "The acme of skill is to defeat the enemy without fighting." This widely-accepted mantra has not yet influenced how we structure our military force packages.

10. Lee Felsenstein of the Interval Research Corporation is the originator of the term "information commons."

11. Over the years authoritative speakers including Mr. Ward Elcock, Director of the Canadian Security and Intelligence Service; Dr. Gordon Oehler, then Director of the DCI's Non-Proliferation Center, and many others have generally agreed that even for topics as seemingly difficult as terrorism and proliferation, open sources of information comprise roughly 80 percent of all-source solution. In fact open sources can contribute as little as 10-20 percent, mostly targeting assistance for denied area coverage by classified sources, and as much as 95-99 percent, strategic economic intelligence. The official National Foreign Intelligence Board finding, based on input from the Community Open Source Program Office, COSPO, is that the U.S. Intelligence Community, and most specifically the Central Intelligence Agency, spends 1 percent of its total budget on open sources, and for this amount of money receives 40 percent of its input to the all-source process.

12. This chart is adapted from materials developed by Dr. Jack Davis, recently retired ean of the Centray Intelligence Agency analysts, whose course, "Intellience Successes and Failures," was the model for the Harvard Intelligence Policy Seminar. A longer discussion of influences on the policymaker and obstacles to informed analysis and informed consumption is available in the author's "A Critical Evaluation of U.S National Intelligence Capabilities," *International Journal of Intelligence and Counterintelligence*, Summer 1993.

13. The author was Special Assistant and Deputy Director of the USMC Intelligence Center from its inception in 1987 through 1992. Early on the author worked with a team to define the Marine Corps model for analysis. A copy of the model, and of the strategic generalizations resulting from the model applied to 69 countries of interest to the Marine Corps, is available in *Open Source Intelligence Handbook*, Joint Military Intelligence Training Center, October 1996. The over-all process has been described in "Intelligence Support to Expeditionary Planners," *Marine Corps Gazette*, September 1991.

14. In his final year as Secretary of State, Warren Christopher unequivocally elevated the environment to the high table of national security. Undersecretary of State Wirth was influential in this matter, principally through the EARTHMAP Report in October 1995, an inter-agency endeavor of over a year's duration which concluded that sustainable development and many other key U.S. policies required accurate global geospatial data for the entire planet. Secretary Christopher was following in the footsteps of Secretary of State James Baker, who noted in his 1989 confirmation hearings the urgent need to increase emphasis on the environment.

15. General Phil Nuber, then Director of the Defense Mapping Agency, attempted—without lasting success—to get the theater commanders to evaluate their contingency plans using the established C-1 to C-4 status reporting system. Most theaters would get a failing grade on most plans because they are not being held accountable for planning the future supply of information and maps in the same way that they must plan for men, materiel, and munitions.

16. Mr. Kerr, former Deputy Director of Central Intelligence and former Director of Intelligence for the CIA, was speaking at OSS '97, "Global Security & Global Competitiveness: Open Source Solutions," in Washington, DC, on September 5, 1997.

17. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, March 1, 1996.

18. The author was one of four people testifying to the Commission on open-source options. At the end of the day, a Thursday, the author was invited to participate in an exercise now known as "the Burundi Exercise," in which all available information from the U.S. Intelligence Community on Burundi was compared with what the author was able to mobilize from private sector sources over the week-end. At 10:00 a.m. on the following Monday, the Commission had received:

- **From Oxford Analytica,** a series of two-page executive reports drafted for their global clients at the Chief Executive Officer level, outlining the political and economic ramifications of the Burundi situation;

- **From Jane's Information Group,** a map of Burundi showing the tribal areas of influence; a 1-page order of battle for each tribe; and a volume of one-paragraph summaries with citations for all articles about Burundi published in the past couple of years in *Jane's Intelligence Review*, *International Defense Review*, and *Jane's Defense Weekly*.

- **From LEXIS-NEXIS,** a listing of the top journalists in the world whose by-line reporting on Burundi suggested their intimate familiarity with the situation;

- **From the Institute of Scientific Information, ISI**, in Philadelphia, a listing of the top academics in the world publishing on the Burundi situation, together with contact information;

- **From East View Publications in Minneapolis,** a listing of all immediately available "Soviet" military topographic maps for Burundi, at the 1:100,000 level.

- **From SPOT Image Corporation, USA,** it was determined that SPOT could provide digital imagery for 100 percent of Burundi, cloud-free and less than 3 years old, at a 10-meter resolution adequate for creating military maps with contour lines at the 1:50,000 level as well as precision-munitions guidance packages and nape of the earth interactive aviation and ground mission rehearsal simulation packages.

The above effort has received wide recognition among those who are responsible for oversight of the U.S. Intelligence Community, and was described by one senior Hill staff manager as "John Henry against the steel hammer—only John Henry won." In fact, it is very important to stress again and again that open sources are *not* a substitute for spies

and satellites. But common sense and fiscal realities suggest that the policymaker be able to exploit open sources to the fullest in their public diplomacy, military acquisition, and economic competitiveness roles, while relying on classified intelligence—classified intelligence presented in the *context* of open sources—for those unique insights and details which cannot be obtained through other means, and which in fact are demonstrably so precious as to warrant the risk and cost of espionage.

19. The Website http://www.oss.net offers the public, at no cost, over 5,000 pages from over 500 authorities that have spoken at the six previous open source intelligence conferences sponsored by the author. Included at this site are abridged versions of the Open Source Intelligence Handbook, the Open Source Intelligence Reader, and eight formal lessons on open source intelligence.

20. Based on official NIMA briefings at the unclassified level.

21. As was widely discussed in official circles at the time, General Nuber had to make a personal appeal to General Norman Schwarzkopf for realignment of national imagery assets to collect precision points with which to make maps. At the same time, the U.S. Air Force gave up on national imagery as its main source of wide-area surveillance and targeting imagery, and began buying vast quantities of commercial imagery directly—without DMA assistance or coordination.

22. Mr. Doug Smith, Deputy Director of NIMA, stated in 1996, at the fifth international symposium on "Global Security & Global Competitiveness: Open Source Solutions," that an estimate of $250 million a year was on the mark. In 1997 he revised this estimate upward toward $500 million a year. Despite his best efforts, however, neither DoD leadership nor the Executive Office of the President are willing to address this critical deficiency—and NIMA as a body has gone so far as to stonewall the *EARTHMAP Report* of October 1995 in which Undersecretary of State Wirth, among other leaders of the civilian elements of government, called for rapidly acquiring global geospatial data at this level of accuracy and detail. The obstacles appear to be twofold: a real ignorance at the theater level about the utility of existing SPOT IMAGE capabilities, and a real reluctance by the Office of the Secretary of Defense to buy commercial imagery from a French source—which prefers instead to wait for the constantly postponed offering of U.S. commercial imagery at the one-meter level of resolution (the author believes this will not be available to the degree SPOT IMAGE data is until about 2010). At the same time, everyone except EAGLE VISION aficionados continues to ignore the fact that one-meter imagery comes with enormous bandwidth, storage, time of

transmission, and cost burdens which we cannot afford in the foreseeable future. One-meter is a "designer" image option, not an industrial image option.

23. "Eyes Wide Shut" was the editorially assigned title for an article about this matter in *WIRED Magazine*, August 1997. The author's complete views on this grave deficiency were articulated in a presentation to the Third Congress of the North American Remote Sensing Industries Association titled "Exploring the Four Pillars: Government, Community, Market, and the World," Washington, DC, May 22, 1997. A copy of the speech outline is available at http://www.oss.net under Documentation/Speeches.

24. Paul Strassmann, former Director of Defense Information and former Chief Information Officer of the Xerox Corporation, among others, has published widely in the information management arena. He estimated that $22 billion could be saved over 7 years by instituting improved management of legacy and new systems. The author estimates that an equal or greater savings could be achieved by similar reforms on the content side—reforms intended to lead to more informed policy-making, acquisition management, and command planning.

25. "The National Security Act of 1992," *American Intelligence Journal,* Winter/Spring 1992, provides a side by side comparison of the changes recommended by the House and the Senate.

26. Mr. Paul Walner, the first Open Source Coordinator for the DCI, coined this term, and intended to emphasize what the Commission on Intelligence subsequently endorsed: that classified capabilities should be called upon only when the intelligence needed cannot be obtained by other means—through open sources.

27. The formal internal paper now in circulation with UK MOD is titled "Proposals for the Development of an Open Source Programme to Support NATO and PfP Activities." The author, Captain Patrick Tyrrell, British Royal Navy, now serves as Commandant of the Defence Intelligence and Security School. Captain Tyrrell earned his OBE for work with NATO leadership, and has an intimate understanding of NATO operational and intelligence capabilities and requirements in relation to the Partners for Peace.

28. Mr. Douglas Dearth has coined this latter term, with the intent of emphasizing that the traditional term is one-dimensional, on a single plane.

TERRORISM AND ASYMMETRY

Stephen Sloan

Introduction.

The profound changes in the international political arena coupled with the equally significant transformation of warfare created by technological change have forced military strategists and planners to reassess the future conflict environment. The accompanying revolution in military affairs (RMA) has called for the development of doctrine that can anticipate and therefore effectively react to future conflicts. At the same time the RMA seeks to develop doctrine that is proactive and can take the operational initiative against present and future adversaries.

The problem of adjusting to new realities is endemic in the long history of warfare. Therefore, an assessment of new challenges and concomitant innovations must not only be viewed in terms of change, but also continuity. For doctrine associated with future warfighting should not be grounded solely on what appears to be the unique elements of contemporary and future warfare. The quest for understanding what appears to be unique may ignore the valid benefits of hindsight gleaned from an understanding predicated on recognizing and applying the lessons that can be learned from the past and modifying and applying them to present and future realities.

The present focus on asymmetric warfare is a manifestation of a desire of military thinkers to label and identify major characteristics in the changing conflict environment and develop the capabilities to take the initiative or respond to it. As one author notes,

> asymmetric warfare is a set of operational practices aimed at negating advantages and exploiting vulnerabilities rather

> than engaging in traditional force-on-force engagements. The incentive to engage in asymmetric warfare is usually greatest for the weakest party in defense against a stronger (and often extra-regional) foe. Asymmetric concepts and moves seek to use the physical environment and military capabilities in ways that are atypical and presumably unanticipated by more established militaries, thus catching them off-balanced and unprepared.[1]

It is the purpose of this paper to relate the current concern with major characteristics of asymmetric warfare to a continuing, but also evolving form of armed conflict—terrorism. While there are many definitions, the following three encapsulate the major elements of the threat and act:

- Terrorism can be defined as a purposeful human activity directed toward the creation of a general climate of fear designed to influence in ways desired by the protagonist, other human beings, and through them some course of events.[2]

- Terrorism is the threat of violence and the use of fear to coerce, persuade and gain public attention.[3]

- Political terrorism is the use, or threat of the use, of violence by an individual or group, whether acting for or in opposition to established authority, when such action is designed to create extreme anxiety and/or fear inducing effects in a target group wider than the immediate victim with the purpose of coercing that group into acceding to the political demands of the perpetrators.[4]

The following discussion will focus on the relationship between a asymmetric warfare and terrorism by addressing four areas of inquiry: (1) Similarities and continuities between asymmetric warfare and terrorism, (2) Discontinuities created by the impact of a transforming international conflict environment and technological change, (3) Implications of both continuity and change as they relate to doctrinal development and the operational

art, and (4) Implications of the relationship between asymmetric warfare and terrorism in the formulation of U.S. security/military policies and strategies.

Similarities and Continuities Between Asymmetric Warfare and Terrorism.

In addressing continuities and changes of terrorism, it is first important to identify the major characteristics of terrorism. By so doing one can then address how these characteristics have both remained constant and changed as a means of understanding the present and future threats of terrorism as an aspect of asymmetric warfare.

In its long history, terrorism has often been viewed as the weapon of the weak directed at a stronger adversary. Thus for example, the

> zealots, also known as the Sicarii (dagger-wielders), were 1st century A.D. Jewish religious nationalists in the Roman province of Judea who carried out terrorist attacks on Roman officials and Jews considered to be Roman collaborators as well as waging an open insurgency against Rome from 66-70 A.D.[5]

The use of terrorism as the part of the strategy of the underdog has throughout the centuries been employed to justify acts and campaigns of terror based on the view that it is often a weapon of last resort employed by the powerless. This mythology continues as today's terrorists proclaim that they have no choice but to engage in their acts against superior forces, be it a military police force, the state or a more vaguely defined international order. Viewed in this manner, terrorism has and will continue to be utilized and justified as an asymmetrical response to superior force. But this mythology of terrorism often ignores the fact that far more people have been subject to terrorism when the full coercive capabilities of the state are used against its own people. In these instances, "enforcement terrorism" has been far more destructive than the "agitational terror"

directed against the established order.[6] Thus, while the focus of the threat is still largely on "terror from below," the rise of modern totalitarianism has refined with murderous efficiency the capabilities of a state to engage in mass terrorism. But with the development of "state-sponsored terrorism" as contrasted to "state terrorism," the line between "agitational terror" and "enforcement terror" has been increasingly blurred.

A second aspect of the historical continuity of terrorism as an aspect of asymmetrical warfare relates to be ability of terrorists in the terminology of modern warfare to employ their acts as a force multiplier, to amplify and maximize their outwardly limited resources against a stronger enemy. This ability is part of a conscious strategy particularly related to central characteristics of terrorism that often differentiate it from other forms of violence. That is, "Terror is a natural phenomenon, terrorism is the conscious exploitation of it."[7] Or, as one authority succinctly notes: "Terrorism aims, by the use of violence or the threat of violence, to coerce governments, authorities, or populations by inducing fear."[8] As we shall see, the ability of the modern terrorist to engage in a form of fear generation, as contrasted to his predecessors, has been greatly expanded as a result of modern technology.

Those who have engaged in asymmetrical warfare have customarily maximized their often limited resources by seeking to intimidate and test the resolve of the stronger adversary. To the terrorist, the threat or act of violence is not only a form of fear generation, it is often a strategy or tactic which places heavy emphasis on the use of purposeful violence as a form of psychological warfare. As one authority noted,

> terrorism is a form of psychological operations (PSYOP) . . . . Many other characteristics of terrorism are argued by the drafters of competing definitions, but virtually all include words to the effect that acts of terrorism are directed at a target audience and not just the immediate victim. Without this

provision terrorism would be indistinguishable from other acts of violence.[9]

The systematic and purposeful use of fear is therefore a central objective of terrorists as they seek to use both threats and the use of violence to create a sense of vulnerability and alter the attitudes and values of the targeted adversary and its population. Psychological operations have also long been in the arsenal of those who have, for example, practiced asymmetric warfare in an insurgency directed against a more powerful enemy. Particularly in a protracted war, such actions have weakened the resolve of the people on the homefront, often thousands of miles away from the physical battle, but such actions can also physically bring the war home and breach the security of a dominant power. Unfortunately, because of technological changes in the current and future conflict environment, the terrorists now, as we shall see, have the capability to intensify their psychological attacks on a mass audience in ways undreamed of by the most skillful and dedicated terrorists of the past.

In addition to its psychological impact, terrorism has proven to be a very effective form of communication. As in the case of asymmetric warfare in general, terrorism remains a powerful tool to convey a message to an intimidated audience. The Russian anarchists who practiced propaganda by the deed have been replaced by new merchants of disorder who now have the capacity to spread their message to a global audience almost instantaneously.[10]

Finally, the use of agitational terror or terror from below has been associated with the long history of insurgency, where such terrorism is essential in the asymmetrical positions of the insurgents compared to the threatened government. Terrorism is therefore a central element in a particular type of warfare, a form of warfare that has been effective not only against powerful nations. Moreover, as we shall see, it is a form of conflict which does not fit the

American ideal of waging war, particularly now that we face the challenges inherent in being the sole military superpower in a very ambiguous conflict environment. Furthermore, since terrorism is often an aspect of a protracted war, those who employ it test the ability of democratic governments to develop and implement necessary long term counterterrorism policies and associated strategies since continuity may be difficult to achieve as one administration replaces another. Moreover, in the war against terrorism decisive victories are unlikely. Also, the pain threshold of the population to endure casualties of any appreciable numbers may now be limited in a democratic political order. Such considerations raise serious questions concerning the ability of the United States and other open societies to persevere against adversaries in a protracted conflict.[11]

Differences and Discontinuities Between Asymmetric Warfare and Terrorism.

The challenges created by the historical characteristics of terrorism, particularly to democratic political orders, have been exacerbated by the transformational conflict environment and the impact of technological change. The end of the Cold War has destroyed the arbitrary coherence created by superpower competition. The balance of nuclear terrorism, with limits on direct confrontation by Moscow and Washington as a result of the Cuban missile crisis, and with some degree of control by the superpowers over the states they employed to engage in proxy warfare, has been replaced by a disequilibrium created by the emergence of rogue states and would-be regional powers. In the case of the former, there has been a rejection of the rules of the game as practiced by what they perceived to be the remnants of a discredited political order that had been initially imposed by the Western imperial powers. In the case of the latter, the arbitrary boundaries of existing nation-states have been rejected by those who wish to create their own hegemony over a strategic region, motivated by

both revolutionary and religious fervor. Furthermore, there are many new significant players in this more ambiguous international area, all seeking to maximize their capabilities now that they do not feel restrained by the limits placed by the competing superpowers during the Cold War. In addition, the ambiguity has been heightened by the emergence of a wide variety of new actors who have rejected the centrality of the state in international politics. These non-state actors, include

> . . . universal and regional intergovernmental organizations (IGO's), transnational guerrilla and terrorists groups, multinational organizations (MNC's), and a rapidly growing number of nongovernmental organizations in a wide variety of functional areas.[12]

One would also add the very significant growth of both organized and unorganized criminal enterprises that have increasingly filled the power vacuum created by the disintegration of the former Soviet Union and have asserted themselves in the "gray areas—immense regions where control has shifted from legitimate governments to new half-political, half-criminal powers."[13]

The systematic breakdown of the international system has enabled these parties to seize the initiative and use terrorism as an instrument to attempt to maximize their foreign policy objectives. In the face of the existing vacuum and the inability of regional and international political organizations to control or combat them, both new state and non-state actors have and will continue to practice the techniques of what can be called armed diplomacy—diplomacy by intimidation thorough the threat and use of terrorism. The breakdown of the Gulf Coalition, the inability of the United Nations to act decisively, and the reluctance of the United States to act unilaterally against Iraq underscore the fact that a strategy of terrorism, of any type, will increasingly challenge the faltering abilities of a fragile and often divided international community to meet present and future threats and contingencies.

The discontinuity in the international arena that has strengthened the threat and use of terrorism as an asymmetric instrument of armed diplomacy, physical conflict, and foreign policy has further been buttressed by the profound impact of changing technologies. While the impact is both complex and wide-ranging, there are a few major characteristics that will enable terrorists to continue to maximize their capabilities in the immediate future. In the first place, modern terrorists now have the ability literally to engage in global operations. They are no longer limited to utilizing terrorism as a tactic in a territorially based insurgency. As a result of the introduction of commercial jet aircraft, we have witnessed the emergence of "Non-Territorial Terrorism"—a form of terror that is not confined to a clearly delineated geographical area.[14]

In a very real sense, terrorists now have the capacity to engage in what could be called low-intensity aerospace warfare. They have at their disposal what are for all practical purposes human intercontinental delivery systems composed of skyjackers, and terrorists who are carrying out operations thousands of miles away from their base of operations. Even more ominous is the fact that states may increasingly use missiles as part of a terrorist delivery system. And the time will come when non-state terrorists may also develop their own long-term stand-off weapon capabilities. The dangers created by these delivery systems has of course been greatly intensified as a result of what could be called a vicious "revolution in terrorist affairs." With the sarin gas attack in the Tokyo subway system on March 20, 1995, by members of the Aum Shinri Kyo cult, the threshold to mass terrorism had been crossed and the dangers of future chemical, biological, and nuclear terrorism can no longer be viewed merely as future threats. We have now witnessed not only the capability but the willingness of various terrorist groups to literally declare a war against all.[15] This willingness and ability to practice mass terrorism may have modified Sun Tzu's edict from

"kill one person, frighten a thousand" to "kill a thousand, frighten a million."

The ability of terrorists to spread fear and intimidation and dramatize their cause to a far stronger adversary as an aspect of asymmetrical warfare has of course been greatly heightened by the impact of the media. We have witnessed the development of the CNNDrome where acts of terrorism and the justification for them can almost immediately reach a global audience.[16] This capability unfortunately has now been enhanced not only through the sophisticated exploitation of the mass media, but increasingly via the internet. It can be anticipated that a terrorist group will skillfully use the net to intimidate a vast new audience by creating the perception of a terrorist act or terrorist campaign even though it might not really exit. We may see the resort to what could be called virtual terrorism, which could have a profound psychological effect on a public that is increasingly willing to seek answers to complex questions by relying on electronic tabloids as a means of creating and reinforcing accompanying conspiracy theories.[17]

The potential development of virtual terrorism can be placed in the broader context of what has now been identified as "information warfare . . . any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting us against those actions; and exploiting our own information functions."[18] Even more specifically, one can identify and address the challenges created by what a number of authors have defined as:

> Information terrorism [which is] the nexus between criminal informations system fraud or abuse, and the physical violence of terrorism. . . . [P]articularly in a legal sense, information terrorism can be the intentional abuse of a digital information system, network, or component toward the end that supports or facilitates a terrorist campaign or action.[19]

Given the profound changes in the international conflict environment and concomitant changes in technology, the challenges created by terrorism as an aspect of asymmetric

conflict will severely test the abilities of the United States and an increasingly fragmented international community to develop the strategies, policies, capabilities, and most importantly the will to combat an ancient form of violence that is also as current as today's headlines.

Doctrinal Development and the Operational Arts.

The challenges created by terrorism as an aspect of asymmetric warfare will require bold and innovative measures to counter a form of violence which will increasingly threaten U.S. national security and Washington's present role as the sole remaining military superpower. The following factors should be considered in developing the ability not only to react, but to take the initiative against potential adversaries who can convert their relative weakness to a source of strength and in so doing transform U.S. strength into a source of weakness.

The ambiguity that now characterizes the international arena also characterizes the nature of terrorism. While there may be agreement on its essential characteristics, there remain understandable debates whether terrorism is first and foremost a criminal act, a form of political violence or ultimately a form of warfare. The fact is that terrorism spans the spectrum of violence, conflict, and warfare. It is multifaceted, a consideration that places an onerous burden on those who would evolve doctrine to combat it.

If terrorism is viewed to be primarily a criminal act, it falls under the purview of law enforcement. When the responsibility is placed in the context of democratic law enforcement, counterterrorism measures would focus on prevention and response and only when necessary the utilization of force. In contrast, if terrorism is primarily perceived to be an aspect of warfare, the application of offensive measures combined with the use of maximum force may be viewed as appropriate. Finally, between both poles is the view that terrorism is essentially a form of political violence regarding which a mixture of both

diplomacy and force may be employed to achieve strategic objectives. However, the nature of terrorism is characterized, one thing is clear. In combating terrorism there is a requirement to achieve unity of effort by integrating police, military, and political counterforces to prevent, respond, or take the initiative against terrorism. One should also add that with the emergence of non-state actors who may use terrorism in pursuit of their goals, any counterterrorism measures must increasingly utilize assets from the corporate or private sector. The monopoly of force is not solely in the hands of states. Therefore, as in the case of the present war on drugs, there is no clearly identifiable organization to engage the adversary. The requirement for coordination among often highly specialized and competitive organizations within and outside the organizations traditionally involved in protecting and promoting national security requires a high degree of coordination among outwardly disparate forces. This need for coordination is particularly crucial when terrorism is used as an aspect of asymmetrical conflict.[20]

Furthermore, the challenges created by terrorism have serious implications in regard to developing the appropriate organizational doctrines and capabilities to combat the threat. One of the major characteristics of a larger, more powerful organization is its complexity and specialization of function. Whether it be in the conduct of the affairs of state, the implementation of a criminal justice system, or waging war, there are highly diverse forces outwardly on the same team, but which have their own tactics, strategies, and objectives. In contrast, weaker or smaller entities may lack the resources and accompanying capabilities to have the luxury of specialization. While outwardly a potential liability, the benefits of simplicity may be a real advantage in conflict against a more powerful adversary. Through their simplicity, they may avoid the daunting challenges inherent in coordinating the activities of diverse and complex bureaucratic structures that characterize modern police, security, and military forces. Moreover, the

asymmetric terrorist organization may also avoid the daunting tasks associated with developing effective command, control, and accountability among competing bureaucratic structures. In combating terrorism, particularly as an aspect of asymmetric warfare, simplicity is a necessity for the adversary and often an impossible goal to be achieved by the superior power. Bureaucratic bloat, the differentiation between line and staff functions, turf battles, and endless reorganizations have often been the hallmark of complex organizational responses to terrorism. If the battle is to be effectively joined against terrorism as an aspect of asymmetric warfare, an organizational culture of simplicity may be required even in an ever more complicated technological environment. But achieving simplicity may unfortunately be a highly complex process as a result of the great interdependency and complex organizational arrangements that are the features of modern nation-states and particularly a superpower.

Directly related to the need for simplicity in engaging in asymmetrical warfare are the crucial challenges associated with organizational doctrine, which "is *very* narrow in scope and tends to change relatively frequently in order to remain current."[21] Unfortunately, the doctrine of large-scale complex organizations stresses the requirement for a

> ladder system [which] often acts as a barrier to fast communication and execution of operations with its emphasis on command hierarchy, the differentiation between staff and line function, [and] the problems of coordination with often competing hierarchies.[22]

This organizational doctrine stands in marked contrast to the internal organizational structure of terrorist groups: "The centrifugal infrastructure [which] resembles that of a solar system in which the leader is the sun in the center and the members are like planets around his direct impact."[23] The need to develop a centrifugal organizational structure to maintain counter-cadre to combat those who have a centrifugal terrorist infrastructure is not easy to achieve,

especially when one may require joint operations. Moreover, the requirements for effective command and control as well as the demand for accountability may act as serious impediments when a complex large organization seeks to mirror the organizational structure of those who engage in asymmetrical warfare.

In meeting the asymmetrical threat the key role of simplicity of organization should be joined with yet another doctrinal and operational requirement. That is, in seeking to engage a small, invisible, flexible adversary, the larger power must rely heavily on the key role of intelligence. Since terrorists, whether they are pursuing limited objectives or engaging in a form of warfare, have the initiative to target a vast constellation of targets, authorities are inherently placed on the defensive. Furthermore, target hardening, however effective, is essentially a form of target displacement since the terrorists have the option of seeking softer targets of opportunity.

There are unfortunately many vital targets in a complex, technologically interdependent society. Intelligence can thus be viewed as being on the forefront of counterterrorism warfare. For, once the terrorists go tactical (i.e., initiate operations and move to the target), the authorities are essentially forced into a reactive crisis-emergency management mode with its emphasis on rescue, recovery, damage control, and reconstitution. Therefore intelligence is central in preventing, deterring, and when feasible preempting acts of terrorism. However in meeting the demand of terrorism as a form of asymmetric warfare, one might suggest that there are two outwardly contradictory requirements in regard to both collection and analysis. On one hand, the need for simplicity that characterizes terrorist organizational doctrine is also applicable to counterterrorism collection and analysis. The focal point for such efforts requires the use of HUMINT in the demanding task of penetrating terrorist groups, their fronts, and when appropriate their state-sponsors. As one authority aptly notes,

> HUMINT agencies can try to recruit agents in secretive states where intelligence otherwise has no access. In the same way informers provide almost the only means of penetrating non-state terrorism: and security intelligence has always needed informers on subversive movements and other internal threats.[24]

In conjunction with this is the need to emphasize the training and utilization of area specialists who have the language and associated training and field experience to literally understand the perception and attendant motivation of highly diverse men and women representing different ethnic, political, and religious groups that may resort to terrorism as part of their strategic goals—be they based on the call for self-determination or profit. Unfortunately, and in contrast to the requirement for simplicity, is the consideration that the United States may have placed too much emphasis on sophisticated techniques of technical collection and associated analysis.

In a sense the community may have become to a degree technologically muscle-bound, relying too heavily on high-tech capabilities to penetrate and understand the motivation, behavior, tactics, and strategies of the often small, free-floating combat cells that characterize many contemporary terrorists groups. The most impressive capabilities of overhead platforms and signal intercepts may be relatively useless when confronted with the reality of face-to-face communication by two terrorists who are hiding in a "safe house" in the urban jungle of a city. Yet, at the same time, the need for more sophisticated technical collection has understandably been expanded, given the increased ability of terrorists to use modern technology in the form of communications and weapons to achieve their goals. Hence, in the changing terrorist threat environment there will be a need for the mixture of traditional human collection as well as high-tech alternatives. But the ability to achieve an integration of effort by both may be limited as a result of their different biases based on their training and education. In effect the traditional "green door" barrier

between the operator and analyst may now have been replaced by the barrier between those who emphasize the requirement for the low-tech human-intensive capabilities, on one hand, and high-tech proponents in the intelligence community, on the other. In the increasingly ambiguous world of terrorism where cults, extremist groups, and criminal enterprises of all sorts may act independently of each other, where there are not clearly defined and readily defined targets of collection, where communication may be highly personal and therefore not vulnerable to intercept, there are no technological "silver bullets" for penetration purposes. Therefore, when confronted with the threat of terrorism in asymmetrical warfare, the dominant power must develop the capacity to create and utilize relatively simple organizational structures and not place undue reliance on high-tech measures against enemies who know the value of simplicity in the pursuit of their objectives. This transformation is not easy for the modern administrative state which places heavy value on an organizational structure and culture characterized by complexity. In the asymmetrical conflict against terrorism, the "War of the Flea"—one does not engage in overkill by relying on sophisticated weapon systems.

Implications in Regards to National Security Policies and Strategy.

The challenges created by terrorism placed in the broader context of asymmetric warfare are a manifestation of a profoundly changing conflict environment faced by the United States as the sole remaining military superpower. While there is continuity in regard to applying the lessons of the past to counterterrorism, the new dimensions of terrorism created by the interaction of the revolution in technology and the transformation of the international arena will place a heavy burden on the United States in addressing present and future security requirements. A number of key issues can be identified.

With the end of the outward coherence created by the Cold war it is now very difficult to identify major strategic threats to U.S. national security. The balance of nuclear terrorism and the need for effective deterrence has been replaced by a laundry list of current threats: terrorism, weapons of mass destruction, the international drug trade, global criminality, and other immediate challenges. While these threats are certainly real, they have not been integrated into a long-term strategy. What may be identified as strategy today is for all intents and purposes contingency-driven short-term geopolitical responses to immediate threats. This lack of a long-term strategic vision is further exacerbated by the loss of clarity on what are the major elements of national security. In the past there was a relatively clear identification of such major factors as the Soviet threat and the military, economic, and political dimensions of superpower competition. Now elements of national security have been expanded to include such topics as environmental dangers and other non-traditional threats. It is not that environmental degradation is of trivial concern, it is just that the list has been expanded to make the elements of national security so diffuse that it is difficult to focus, much less establish the clarity needed to establish a strategy.

The lack of clarity has created a situation where those forces involved in protecting national security and advancing American interests have been overwhelmed with a wide variety of new roles and missions under what has been called "operations other than war." Thus, for example, the military, while still confronted with the challenges created by conventional war in the Middle East and Korea, must also address a whole host of new tasks: peacekeeping, peace enforcement, humanitarian assistance, drug enforcement, and other similar demands at the very time when the drawdown in personnel and material continue.[25] Furthermore, the line between military and non-military operations has blurred now that we have witnessed the trend whereby the police acquire military equipment and

training to counter a more demanding criminal challenge, while the military has become increasingly involved in law enforcement operations as illustrated by its "war on drugs" and border interdiction of illegal immigrants. We are witnessing what may be called "The Militarization of the Police and the Gendarmification of the Military."[26] With a lack of a clearly enunciated strategy and with a bewildering myriad of roles and missions that imperfectly fuse military and law enforcement functions, it is no wonder that the United States is ill prepared to deal with both the short- and long-term threats to national security created by those who are and will engage in asymmetric warfare.

The lack of vision has also manifested itself in the realm of national policy. With the end of the Cold War, whatever bipartisan consensus that remained was greatly weakened as both Congress and the Office of the President turned inward to meet domestic concerns without a long-term commitment to the formulation and execution of foreign policy. It should come as no shock to discover that it is exceedingly difficult to formulate long-term strategy in a policy vacuum. This vacuum creates particular problems in developing appropriate measures for combating terrorism as an aspect of asymmetric war. As noted earlier, terrorism has traditionally been viewed as a form of protracted warfare in which there are few decisive, much less total victories. The terrorist who engages in asymmetric warfare against a greatly superior power has time on his side, for he can focus operations to create a maximum amount of disruption and instability with a minimum number of personnel, resources, and weapons.

Moreover, with the advent of mass terrorism, terrorists can further maximize their capabilities with frightening efficiency. Hence, there are serious questions whether the current and future political leadership, policymakers, and indeed the public have the necessary vision, capability, and, perhaps most importantly, the resolve to maintain the strength of will necessary to deal with adversaries who are skilled and committed to engaging in protracted war. The

American ideal of waging war which calls for minimum casualties, decisive outcomes, and short conflicts unfortunately does not match the reality of the current and future conflict environment. Terrorism, be it conducted by a small ethnic group as part of a regional program of destabilization, or solely for profit, will severely test the ability and staying power of the United States to meet the "death of a thousand cuts" that is often the hallmark of protracted conflict.[27] Furthermore, terrorists have and will increasingly use the media and modern technology not only bring to the war home to the American public, but to test that public's will to confront the threat. In "The War in the Shadows" where stealth and protraction often go hand in hand, American staying power is open to question.

Further complicating the challenge faced by the United States is the fact that in the next century, Washington will no longer be the sole military superpower. Consequently more than ever there will be the requirement for the United States to act in coalition with other parties against a whole variety of new threats. But this will in all probability become even more difficult since we live in an international environment that, while more economically and technologically interdependent, may have also become more politically divided. We could witness the appearance of a wide variety of groups that reject any semblance of an international political order. Viewed in this light, asymmetric warfare will not only continue, but may even become more threatening to a fragile international order where the possession of political and economic power may be transformed into a liability—a target rich environment for terrorists to practice their form of asymmetric warfare.

Conclusion.

Terrorism is but one manifestation of asymmetric warfare. But it is a manifestation that in all likelihood will increasingly challenge the United States in the next century. Changes in doctrine, strategy, and policy are

needed, but it is difficult for a superpower to think organizationally small, breaking through the complexity of modern government to look beyond the current threats and formulate a new strategic vision in a rapidly changing international arena. Terrorism and asymmetry serve to underscore the need to move beyond the conventional wisdom of today—a wisdom that will mean far less in a conflict environment where mass society and high technology compete with parochial loyalties and the low-tech forms of violence, thus intensifying instability in an international arena already characterized by disunity and uncertainty.

ENDNOTES

1. Paul F. Herman, Jr., "Asymmetric Warfare: Sizing the Threat," *Low Intensity Conflict and Law Enforcement*, Vol. 6, No. 1, Spring 1997, p. 176.

2. H. H. A. Cooper, *Evaluating the Terrorist Threat: Principles and Applied Risk Assessment,* Clandestine Tactics and Technology Series, Gaithersburg, MD: International Association of Chiefs of Police, 1974, p. 4.

3. National Advisory Committee on Justice Criminal Standards and Goals, *Report of the Task Force on Disorders and Terrorism*, Washington, DC: U.S. Government Printing Office, 1976, p. 3.

4. Grant Wardlaw, *Political Terrorism: Theory, Tactics and Counter-Measures*, Cambridge: Cambridge University Press, 1982, p. 16.

5. Sean Anderson and Stephen Sloan, eds., *Historical Dictionary of Terrorism,* Metuchen, NJ: Scarecrow press, 1995, pp. 371-372.

6. Thomas B. Thornton, "Terror as a Weapon of Political Agitation," in Harry Eckstein, ed., *Internal War*, New York: The Free Press, 1964, pp. 71-91. Also, for a good overview of state terrorism, see: Raymond D. Duvall and Michael Stohl, "Governance by Terror," in Michael Stohl, ed., *The Politics of Terrorism*, Third Ed., Revised and Expanded, New York: Marcel Dekker, Inc., 1988.

7. National Advisory Committee on Criminal Justice Standards and Goals, *Report of the Task Force on Disorders and Terrorism*, Washington, DC: U.S. Government Printing Office, 1976, p. 3.

8. Richard Clutterbuck, *Guerrillas and Terrorists*, London: Farber and Farber, Ltd, 1977, p. 21.

9. Michael T. McEwen, "Psychological Operations Against Terrorism: The Unused Weapon," *Military Review*, January 1986, p. 62.

10. For a brief discussion, see James M. Poland, *Understanding Terrorism: Groups, Strategies and Responses*, Englewood Cliffs, NJ: 1988, pp. 34-36.

11. For an excellent discussion on the strategy of terrorism in unconventional war, see Bard E. O'Neill, *Insurgency and Terrorism: Inside Modern Revolutionary Warfare*, New York, NY: Brassey's Inc., 1990.

12. Maurice A. East, "The International System Perspective and Foreign Policy," *Why Nations Act: Theoretical Perspectives in Comparative Foreign Policy Studies,* Maurice A. East, *et. al*., eds., Beverly Hills, CA: Sage Publications, 1978. p. 145.

13. Xavier Raufer, "Gray Areas: A New Security Threat," *Political Warfare: Intelligence, Active Measures and Terrorism Report*, Spring 1992, p. 1.

14. Stephen Sloan, *The Anatomy of Non-Territorial Terrorism: An Analytical Essay*, Clandestine and Technology Series, Gaitherburg, MD: The International Association of Chiefs of Police, 1978, p. 3.

15. For an excellent account of the Tokyo attack and a previous attack in the Nagano Prefecture as well as a chilling description and analysis of the Aum Shinri Kyo Cult, see D.W. Brackett, *Holy Terror: Armegaddon in Tokyo*, New York, NY: Weatherhill, Inc., 1996.

16. The term CNNDrome was coined by Lieutenant Colonel David G. Bradford in *The Shadow Falls: The Gray Area Phenomenon in Today's World*, unpublished manuscript.

17. Pierre Salinger's theory on the bombing of TWA 800 still has electronic legs on the Internet where it was initiated, and there is no reason to believe that the line between "real" and "virtual" terrorism might not be blurred in the future.

18. *Cornerstones of Information Warfare*, Washington, DC: Department of the Air Force, 1966.

19. Matthew G. Devost, Brian Hougton, and Neal A. Pollard, a paper entitled "Information Terrorism: Can You Trust Your Toaster?" 1996, p. 10. Also see the revisions in their article "Information Terrorism: Political Violence in the Information Age," *Terrorism and Political Violence*, Spring, 1997.

20. Roberto Suro, "U.S. Lacking in Terrorism Defenses," *The Washington Post*, April 24, 1998, pp. A6, A18.

21. Lieutenant Colonel Dennis M. Drew, USAF, "Of Trees and Leaves: A New View of Doctrine," *Air University Review*, January-February 1994, p. 44.

22. J.K. Zawodny, "Infrastructures of Terrorist Organizations," *Conflict Quarterly*, Spring, 1981, p. 26.

23. *Ibid.*, p. 24.

24. Michael Herman, *Intelligence Power in Peace and War*, The Royal Institute of International Affairs, Cambridge: Cambridge University Press, 1996, p. 65.

25. For a current discussion of Operations Other Than War, particularly in reference to the role of special forces, see Colonel Ed Phillips, "Army SOF: Right Tool for OOTW," *Special Warfare*, Summer, 1997.

26. Stephen Sloan, *Changing Roles: The Militarization of the Police, The Gendarmification of the Military and the Privatization of Security—A Challenge to the Democratic Order,* unpublished manuscript. For an excellent discussion of the changing role of the police in the conduct of international affairs, see Robert Oakley and Michael Dziedzic, "Policing the New World Disorder," *Strategic Forum*, October, 1996.

27. For an excellent discussion on American values associated with waging war, see Donald Vought, "American Culture and American Arms," *Lessons From An Unconventional War: Reassessing U.S. Strategies in Future Conflicts*, Richard A. Hunt and Richard A. Shultz, Jr., eds., New York, NY: Pergamon Press, 1982.

METAPHORS AND MODERN THREATS: BIOLOGICAL, COMPUTER, AND COGNITIVE VIRUSES

Edmund M. Glabus

INTRODUCTION

One challenge of national security planning and force protection programming is how to visualize military threats. For current operations, this task is made difficult by the sheer volume of information we receive purporting to help us understand threats to military and civilian assets and operations. Unfortunately, military decisionmakers, planners, and analysts are often exposed to more information about any given situation than they can assimilate within normal operational time constraints. When planning for future strategies and capabilities, the converse is true. Instead of too much information, we suffer from too little. Analysts, planners, and leaders understandably are hesitant to "bet the farm" on predictions, projections, or forecasts about future adversaries and scenarios.

However, time and events wait for no man. In the short term the budget calendar, Program Objective Memorandum (POM) timeline, and systems acquisition and fielding cycles all drive Department of Defense personnel to identify assumptions, derive conclusions, present recommendations, and make decisions. The military leadership's emphasis on extending our conceptual horizons (e.g., *Joint Vision 2010*, *Army 2010*, the Army After Next Project) also impels us to complete similar actions with even less clarity and confidence in our assessments. As a result many decision-makers, planners, and analysts use only a few highly representative pieces of information to reduce problems to a manageable size.

In the complicated environment of military strategy, decision-makers and staffs will use these shortcuts, or heuristics, to classify situations according to a few key features and guide their thinking (and learning). There is nothing inherently wrong with this shortcut approach to planning and decisionmaking as long as our heuristics are reasonably representative. One favorite technique is the use of the metaphor. As Martin Libicki writes,

> Used properly, a metaphor can be a starting point for analysis, a littoral, as it were, between the land of the known and the ocean of the unfamiliar. A good metaphor can help frame the questions that might otherwise not arise, it can illustrate relationships whose importance might otherwise be overlooked, and it can provide a useful heuristic device, a way to play with concepts, to hold them up to the light to catch the right reflections, and to tease out questions for further inquiry.[1]

One useful metaphor we can use to visualize modern threats is that of the virus. Most of us have some familiarity with viruses. Usually we are aware of related terms like vaccine, inoculation, and antibiotic. Viruses are mysterious creatures to some, but reference to virus threats has achieved a degree of acceptance in national security discussions. Two developments contributing to this acceptance are the recent emphasis on information warfare/information operations, with a strong focus on computers, and an unfortunate resurgence in biological warfare activities on both the international and domestic scenes.

Before we can discuss using viruses as a threat metaphor, however, we need to define the term in a conventional sense:[2]

> vi-rus…[L, slimy liquid, poison, stench….]
> 1: archaic: venom emitted by a poisonous animal
> 2a: the causative agent of an infectious disease : disease germ
> 2b: FILTERABLE VIRUS; specifically : any of a large group of submicroscopic infective agents that are held by some to be living organisms and by others to be complex autocatalytic

protein molecules containing nucleic acids and comparable to genes, that are capable of growth and multiplication only in living cells, and that cause various important diseases in man, animals, or plants….
2c: VIRUS DISEASE….
3: a morbid corrupting quality in intellectual or moral conditions : something that poisons the mind or soul….
4: an antigenic but not infective material (as vaccine lymph)….

In light of this formal definition, we will explore the use of the virus as a metaphor for discussing threats that are difficult to visualize. We will focus on biological warfare, computer network attack, and memetic warfare (Figure 14). Using the Army After Next (AAN) Project's construct of doctrine/concept/idea,[3] we can view the three types of warfare listed above through the metaphor of the virus in order to present them in an easily understandable way. As we move from biological warfare, to computer network attack, to memetic warfare, our illustrations will cross the spectrum from doctrine, to concept, to idea.

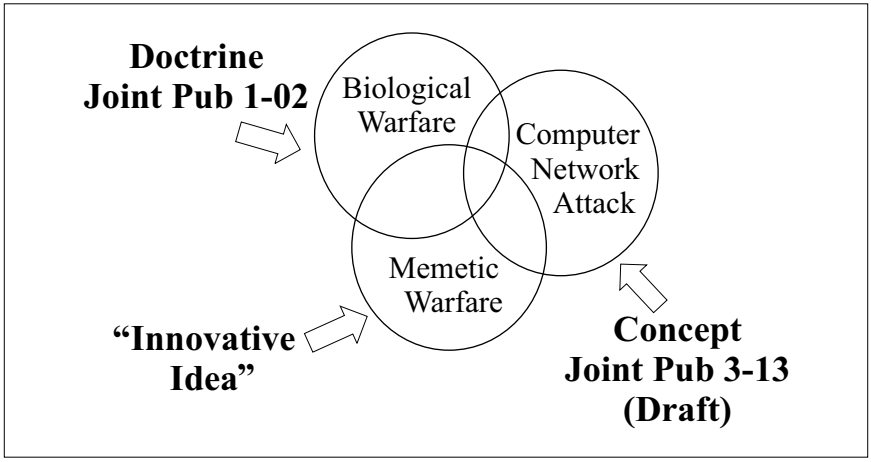

Figure 14. Viruses in the Context of Warfare.

SUMMARY AND RELATIONSHIP OF VIRUS METAPHORS

In his book *Virus of the Mind: The New Science of the Meme*, Richard Brodie relies on metaphor to discuss what he

concludes is a new form of virus. According to Brodie, "viruses occur in three different universes: biology, computers, and the mind." Viruses of the mind we shall refer to as "cognitive" viruses. The following table, adapted from one found in *Virus of the Mind*, "shows the correspondence between words used to talk about evolution and viruses in each of the three universes."[4] In this article we will use Brodie's taxonomy to explore the use of the virus metaphor, examining in turn the use of biological, computer, and cognitive viruses as threat metaphors.

Biology	Computers	Cognition
Gene	Machine Instruction	Meme
Cell	Computer [and Paper]	Mind
DNA	Machine Language	Brain Representations
Virus	Computer Virus	Virus of the Mind
Gene Pool	All Software	Meme Pool
Spores/Germs	Elect. Bulletin Board Postings	Broadcasts/Publications
Species	Operating System	Cultural Institutions
Genus/Higher Classifications	Machine Architecture	Culture
Organism	Program	Behavior/Artifact
Genetic Susceptibility	"Back Door" or Security Hole	Psychological Susceptibility or "Button"
Genetic Evolution	Artificial Life	Cultural Evolution

BIOLOGICAL VIRUSES: DEFINITION AND THREAT CONTEXT

Firmly grounded in doctrine, biological warfare is the "employment of biological agents to produce casualties in man or animals and damage to plants or materiel; or defense against such employment."[5] It is the easiest type of warfare to discuss using the term virus, as viruses literally are part of the discipline. For purposes of this paper, we will use version 2b of the virus definition presented earlier to describe viruses when the term is associated with the biological threat. Although most closely related to the virus metaphor, biological warfare threats include more than viruses (e.g., bioregulators, bacteria, fungal toxins, and vectors). From a layman's perspective, however, these biological warfare threats can all be visualized in terms of viruses.

As with most national security threats, the majority of official government analyses and estimates are classified. However, one particularly good open source document on the biological virus threat is the Office of the Secretary of Defense's *Proliferation: Threat and Response.*[6] In a concise threat statement, the OSD report concludes: "Biological weapons have the greatest potential for lethality of any weapon. Biological weapons are accessible to all countries; there are few barriers to developing such weapons with a modest level of effort. The current level of sophistication for many biological agents is low but there is enormous potential—based on advances in modern molecular biology, fermentation, and drug delivery technology—for making more sophisticated weapons."[7]

The magnitude of the biological warfare threat is difficult to convey, but one example gives an idea of the potential scope of the problem. According to an article by *Washington Post* staff writer R. Jeffrey Smith, Iraq has *declared* it maintained biological weapons, including anthrax, botulinum toxin, and aflatoxin. Let's use only the first two of these agents as examples.

- Anthrax: "This often fatal bacteria causes high fever, difficulty in breathing, chest pain and eventually blood poisoning. Antibiotics often prove useless after a short period. [Iraq has declared] 2,245 gallons, enough to kill billions. The United Nations (U.N.) suspects production was three to four times that."

- Botulinum Toxin: "This bacteria first causes vomiting, constipation, thirst, weakness, fever, dizziness, blurred vision, pupil dilation and difficulty in swallowing. Eventually it causes paralysis, respiratory failure, and often death. [Iraq has declared] 5,125 gallons, enough to wipe out Earth's population several times. The United Nations suspects the number may have been twice that."[8]

Although it is convenient to focus on one country, Iraq is not alone in this respect. The OSD report addresses potential research, production, testing, or weaponization of biological weapons by Iraq, North Korea, China, Iran, and Russia, among others.

Potential non-state actors include both foreign terrorist organizations and domestic groups. Recently in the United States a "microbiologist on probation for fraudulently obtaining bubonic plague toxins in Ohio in 1995, and . . . a Las Vegas area entrepreneur and home-laboratory medical researcher, were arrested . . . [and] charged with possessing anthrax for use as a weapon."[9] Although, as it turned out, the vials contained a harmless anthrax strain for use in inoculating farm animals, FBI agents continued to investigate the potential for criminal wrongdoing. Other examples are more clear-cut. As Charles Mercier writes,

> biological . . . agents can readily be developed by terrorists…[requiring] a college-level knowledge of biology or chemistry, less than $20,000 in supplies, and the forged documents or accomplices needed to obtain "seed" bacteria or precursor chemicals . . . a U.S. neo-Nazi group (the Order of the Rising sun) produced 80 pounds of typhoid bacillus in 1972, and in 1984 Paris police raided an apartment rented by the Baader

> Meinhof gang and found flasks of Clostridium botulinum culture. More recently, Japanese police found 160 barrels of peptone (a growth media for bacteria) along with Clostridium botulinum when they raided an Aum Shinrikyo compound near Mount Fuji. Tricoecene mycotoxins (e.g., "yellow rain") can be produced simply using a corn meal slurry and the appropriate strain of fungus.[10]

In discussions of biological warfare, we can start by examining viruses in a literal sense, as part of the family of biological agents. It is very easy for us to then turn to other biological threats and apply the virus metaphor. However, a more interesting test is to apply the metaphor to information warfare, specifically the realms of computers and cognition.

COMPUTER VIRUSES: DEFINITION AND THREAT CONTEXT

With regard to joint doctrine, computer network attack, after starting out as an innovative idea, is currently undergoing refinement as a concept and appears to be making a formal transition to doctrine. Computer network attack is currently defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[11] It was inserted in the draft of *Joint Publication 3-13, Information Operations*, and has survived the early rounds of staffing. Although computer network attack is not focused solely on defending against viruses ("hacking" without inserting viruses is a constant concern among military information security professionals), computer viruses are certainly a leading threat concern. The U.S. Army's *Field Manual 100-6, Information Operations,* also refers to virus threats, but the treatment is brief: "It is even possible that a military system could come from the factory with an embedded logic bomb or virus. In the past, new commercial floppy disks used by government agencies have been found to contain a virus upon delivery from the factory."[12]

We interpret computer viruses using Dr. Fred Cohen's informal definition: "A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself." [13] It is useful to note that computer viruses do not exist solely in the digital environment. For example the publication *2600* and other magazines (published openly or underground) contain written code for viruses in a "dormant" state, waiting to be input as machine instructions in computer software.

Demonstrating the current threat from computer viruses is difficult for several reasons. In this instance, both the government and industry share a reluctance to discuss and disclose "cyber-threats" and associated attacks. The government, as is common with threat estimates, has based much of its analysis on classified data. Industry on the other hand, while concerned with privacy and proprietary data, is perhaps more driven by the desire not to lose customer confidence by disclosing vulnerabilities and mishaps involving its automated information systems.

The Report of the President's Commission on Critical Infrastructure Protection (PCCIP) represents the most inclusive effort to date to arrive at a baseline unclassified threat statement for computer networks. In addition to the hacking threat, the commissioners specifically mention America's vulnerability to viruses.

> The threat is real enough. . . . Skilled computer operators have demonstrated their ability to gain access to networks without authorization. . . . Whatever their motivation, their success in entering networks to alter data, extract financial or proprietary information, *or introduce viruses* demonstrates that it can be done and gives rise to concerns that, in the future, some party wishing to do serious damage to the United States will do so by the same means.[Emphasis added.][14]

While general information on the threat from viruses is available,[15] more specific public information on deliberate attacks is unlikely to appear unless and until some of the

PCCIP's recommendations for information sharing are implemented.

Our aim, though, is to explore the use of viruses as a metaphor for modern threats. In the context of our metaphor to visualize threats, what if we step back from the actual machine instructions used in computer viruses? Does the virus metaphor apply to the more common hacking threat? Cyber attack in the form of unauthorized entry into a network or system is a serious concern, comprising the chief focus of the PCCIP. One of the more rigorous examinations of the threat of computer attack is a 1996 General Accounting Office (GAO) report. While the report admits the exact number of computer attacks on the Department of Defense is unknown, it goes on to declare that "Defense may have experienced about 250,000 attacks last year [1995], and...the number of attacks is increasing."[16]

The report contains what has become an infamous collection of statistics by the Defense Information Systems Agency (DISA), the implications of which are eye opening for strategists. According to the report, the DISA Vulnerability Analysis and Assessment Program simulates cyber attacks by attempting:

> to penetrate computer systems at various military service and Defense agency sites via the Internet. Since the program's inception in 1992, DISA has conducted almost 38,000 attacks on Defense computer systems to test how well they were protected. DISA successfully gained access 65 percent of the time. Of these successful attacks, only 988 or about 4 percent were detected by the target organizations. Of those detected, only 267 attacks or roughly 27 percent were reported to DISA. Therefore, only about 1 in 150 successful attacks drew an active defensive response from the organizations being tested.[17]

Using version 2b of the definition of virus from this paper's introduction, consider for a moment the nature of these simulated cyber attacks, as well as actual attacks

reported in the news media. There are many types of hackers, who

- can be aggregated by age, motivation, nationality, etc. ("any of a large group of")
- are extremely small in relation to their targets—from one to a handful of hackers taking on several major military installations simultaneously for example ("submicroscopic" in relative size)
- obtain unauthorized and undesirable entry ("infectious agents')
- recruit new members, teach them, and share tools ("are capable of growth and multiplication"), and
- according to the GAO report have caused costly and considerable damage ("cause various important diseases"). Certainly the virus metaphor appears to be a fitting layman's thumbnail denomination for the cyber attack threat. On one level it can be said that infectious agents (hackers) sometimes use infectious agents (viruses) in their cyber attacks.

COGNITIVE VIRUSES: DEFINITION AND THREAT CONTEXT

Perhaps the most challenging type of warfare to relate convincingly to the virus metaphor is memetic warfare, based upon cognitive viruses. This is the case for a number of reasons. First, *memes* and *memetics* are both relatively recent terms in scholarship and national security explorations. Second, by no means are the ideas contained in and accompanying the area of memetics regarded by either academics or strategists as proven. Finally, memetic warfare is the least tangible type of warfare nominated in this paper for serious examination.

The scope of this paper does not permit a full treatment of the idea of memetic warfare. The closest related doctrinal term would be "perception management," defined as

- actions taken to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations.[18]

Fortunately in the context of the Army After Next Project's construct, the nomination of "innovative ideas" like memetic warfare is encouraged. It is when the idea becomes a candidate for an Army concept or doctrine that it undergoes the acid test. In this paper we can merely outline the idea and discuss it in terms of cognitive viruses.

We define a cognitive virus as any agent that infects people with a meme, a unit of information in a mind whose existence influences events such that more copies of itself get created in other minds. Professor Richard Dawkins hinted at the original idea of the meme in his book *The Selfish Gene*, and he defined the term in *The Extended Phenotype*.[19] Several thinkers have extended this idea to discussions of warfare, including the father of modern information warfare, Dr. Thomas P. Rona, who described the idea of "societal immunodeficiency virus" (or SIV, against which unwarned populations would have no effective defenses) in some of his last discussions and writings.[20]

A good but short (3-page) summary of the memetic warfare idea is found in the Jane's Special Report, *U.S. Information Warfare,* by Dr. George Stein and Colonel (USAF Retired) Richard Szafranski. The section titled "The

Memetic Warfare Model" attempts to apply memetics to the topic of information warfare, with very intriguing implications. The authors first recapitulate the tenets of memetics, describing the meme as "the basic unit of cultural imitation. . . . the means by which a society reproduces itself." They also call memes the "monads or building blocks of culture, thinking and behavior," stating that "humans appear to be able to create 'designer viruses' of the mind [that] nature cannot." [21]

Turning to the topic of information warfare (IW), Stein and Szafranski speculate that "IW activities would be designed to . . . insert new memes into the mind of the adversary. In so doing, however, the mind viruses would immediately begin to evolve, as each affected enemy mind added to or modified the deployed virus." According to the authors, if borne out by further research and scientific study,

> In memetic-based IW, overt and subliminal messages could be constructed to communicate memes at multiple levels, aiming to travel at what Colonel [Robert J.] Wood characterized as different "channels."[22] Hidden somewhere in the surrender and safe passage leaflets routinely used to incite enemies to despair and surrender ought to be a snake split in two, a good soldier towering above, an abundance of food and sunshine on the surrender side of the line and a golden bridge across. Where propaganda leaflets fail to use multiple channels, they fail to compound the probability that the right memes are communicated.[23]

We need to point out a chief difference between traditional propaganda and memetic warfare, and introduce a threat context for cognitive viruses. Unlike traditional psychological operations (PSYOP) themes and messages, cognitive viruses by our definition infect people with a meme, a unit of information in a mind whose existence influences events such that more copies of itself get created in other minds. These memes present a potential threat and opportunity for military strategists because they spread so well and are so durable. In America, civilian

examples of these memes are the "bad ideas" that simply won't go away. In *Virus of the Mind,* Brodie illustrates several such as conspiracy theories (to include both "vast right-wing and vast left-wing" themes), urban legends (e.g., decades-old complaints that Procter & Gamble's logo is a satanic symbol), and get-rich-quick Ponzi schemes that continue to draw in victims and make their propagators rich.[24]

While these examples may make for amusing coffee-bar banter, some memes have very deleterious effects, with potential impacts on the overseas environment in which U.S. national security activities (and potential military deployments) occur. During the Korean Conflict, allegations of U.S. germ warfare spread particularly quickly, and proved resistant to repeated American denials.[25] More recently there has been a continuous low-level strain of rumor and innuendo that the CIA and/or DoD invented the AIDS virus, and then exported it overseas as part of a racist plot. Frank Barnett writes that *glasnost* failed to inhibit "Gorbachev's regime from inciting Africans to believe that U.S. defense factories generated the AIDS virus, or from inflaming India with the rumor that Washington hatched the plot to assassinate Mrs. Gandhi."[26] These particularly tenacious memes have yet to be eradicated. For another example, we could ask soldiers who have been stationed in Latin America, specifically those who have traveled to Guatemala, about the enduring local rumors that Americans are buying babies and using them for body parts and medicinal experiments.[27]

We might wonder whether some of these memes are so potent as to be impossible to eradicate, and will continue to require managed treatment in the form of denials and focused public information campaigns when outbreaks flare up. In addition we might ask what the difference is between memetic warfare and perception management. There might not be a difference; perhaps the ideas we described above are only an advanced form of modern perception management, using the best research and analysis

available from area specialists, cultural anthropologists, psychologists, technologists, and communications professionals. On the other hand, it may be that memetics will enable military analysts, planners, and decisionmakers to obtain a greater understanding of IW, providing a potent and refined tool with which to shape our adversaries' perceptions. In that case, the effect may well most resemble the activities of "viruses of the mind," and the virus metaphor would be well chosen.

SUITABILITY OF THE VIRUS METAPHOR

Although we chose the virus metaphor to help visualize modern threats, the technique is not without its pitfalls. Martin Libicki used metaphors as intellectual tools throughout his book *Defending Cyberspace and Other Metaphors*, but he is cautious in prescribing them:

> Before analysis proceeds and policy recommendations can be justified, metaphors must be put back into the box from whence they came so that issues can be understood for what they are, not what they look like. To use metaphor in place of analysis verges on intellectual abuse. It invites the unquestioning extension of a logic that works across the looking glass but lacks explanatory power in the real world. Those who forget this are apt to try to make their metaphors do their thinking for them.

Put another way, when one holds a hammer, most problems look like nails. However, Libicki's metaphors, including a fascinating essay on warfighting lessons to be learned from observing the human immune system,[29] show an appreciation for the judicious use of metaphor.

In the data smog of the modern information environment, decisionmakers, planners, and analysts often use only a few highly representative pieces of information to reduce problems of current operations to a manageable size. The military leadership's emphasis on extending conceptual horizons to the year 2020 and beyond also impels strategists to conduct assessments, present recommendations, and make decisions with even less clarity and

confidence in their assessments. In response, decision-makers and staffs will use shortcuts, or heuristics, to classify situations according to a few key features and guide their thinking (and learning).

The virus metaphor shows promise as a visualization tool to grapple with modern threats in biological warfare, computer network attack, and memetic warfare. Used judiciously, and in particular if coupled with the AAN's construct of doctrine/concepts/ideas, the virus metaphor helps provide both definition and context for harried strategists assembling concise threat pictures. If the metaphor withstands the scrutiny of time and criticism, it may prove a valuable thinking and learning tool suitable for the military's intellectual toolbox.

VIRUSES, WMD, AND ASYMMETRICAL WARFARE

For all our focus on viruses as a metaphor to visualize modern threats, how serious are "virus threats"? Are viruses really weapons of mass destruction (however unconventional)? If so, could the United States be blindsided by their employment?

Weapons of Mass Destruction.

Certainly the potential exists for a "bolt out of the blue" strike employing biological weapons. Their delivery at the proper time and place would almost assuredly cause massive casualties in a highly industrialized nation, with estimates ranging from 100,000 to a million for more serious attacks. Efforts to control them range from international agreements such as the Biological and Toxin Weapons Convention to the U.N. inspection effort in Iraq. Biological viruses are weapons of mass destruction in the most concrete sense, with permanent and complete effects projected to be every bit as lethal as some nuclear weapons.

Weapons of Mass Disruption.

The case of computer viruses, writ small as machine instructions or writ large as hackers, is less clear. Certainly there are those who predict an "electronic Pearl Harbor," a large-scale surprise information warfare strike on America's critical infrastructure. Others acknowledge this possibility, but believe the more likely circumstance to be a large-scale attack without very destructive effects. For a strategic cyber attack, the "modern version of the *scorched earth principle becomes logically the destruction, incapacitation, and corruption of the enemy's information infrastructure.* This aspect of 'information warfare' has the side benefit for the attacker to create confusion, panic, and irrationality among the civilian target population. "[30] In this case, viruses are more like weapons of mass disruption, having a temporary and partial, albeit potentially serious effect. (See Figure 15.)

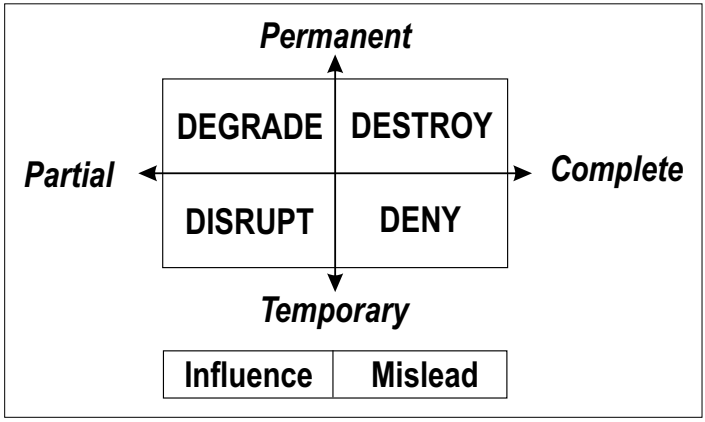

Figure 15. Unconventional Weapons of Mass Destruction/Disruption?

Weapons of Mass Deception.

Finally we turn to the question of cognitive viruses. While some may abhor their use in either peace or war, their employment seems destined to continue, if not increase. It has been argued that what we have called memetic warfare

has been used to instigate outbreaks of violence in Rwanda, Somalia, and the former Yugoslavia. The issue is inflammatory, but the alleged misuse of mass media is sufficiently troubling that recommendations to create a special U.N. unit to "monitor, counter, and block radio and television broadcasts that incited widespread violence in crisis zones around the world" has come from such unlikely sources as a former U.N. Human Rights Officer. However troubling the concept of cognitive viruses might be in some quarters, and recognizing that they can compound if not instigate bloodshed, they are better termed weapons of mass deception than mass destruction.

Rather than thinking of them solely in terms of WMD, a better approach is to recognize that the different types of "virus warfare" are well-suited for use as asymmetrical means in a conflict. Asymmetrical warfare is likely to be one of the foremost challenges faced by the United States in future conflicts. As General Charles Krulak stated, "Our enemies have seen CNN. They watched the technology and they will not be content to fight the son of DESERT STORM. They will fight the stepson of Chechnya, the stepson of Somalia. [The 21st century] will be a century—the first part of it at least—of chaos."[32]

Assessments of AAN wargames have supported General Krulak's assessment. Asymmetrical responses characterized the Red Team's reaction in the face of Blue's superiority in firepower and information dominance: "Red's learning curve rose sharply as the games progressed. Confronted by overwhelming combat power, he resorted to asymmetric responses in an effort to offset Blue's advantages."[33] Just as the notional adversaries engaged in asymmetrical warfare during the wargame, future U.S. adversaries could employ the three types of "virus threats" described above. In thinking through the implications of asymmetrical threats, using the virus metaphor as a visualization tool could assist strategists in this difficult task.

ENDNOTES

1. Martin C. Libicki, *Defending Cyberspace and Other Metaphors*, Washington, DC: Institute for National Strategic Studies, 1997, p. 6.

2. *Webster's Third International Dictionary of the English Language, Unabridged*, Springfield, MA: Merriam-Webster, 1961, p. 2556.

3. *The Annual Report on the Army After Next Project to the Chief of Staff of the Army*, July 1997.

4. Richard Brodie, *Virus of the Mind: The New Science of the Meme*, Seattle, WA: Integral Press, 1996, p. 56.

5. *Joint Publication 1-02, Dictionary of Military and Associated Terms*, Washington, DC: U.S. Government Printing Office, 1989, p. 52. The definition of biological warfare actually says "See Biological Operation," an interesting parallel to current discussions about the relationship between information *warfare* and information *operations*.

6. Office of the Secretary of Defense, *Proliferation: Threat and Response*, Washington, DC: U.S. Government Printing Office, November 1997.

7. *Proliferation: Threat and Response*, p. 81.

8. R. Jeffrey Smith, "Poison, Germ Weapons Would Not Be Direct Targets," *The Washington Post,* February 22, 1998, p. A28. As a point of comparison, the average backyard pool has 25,000 gallons of water. (Source: Customer service representative, Maryland Pools, Inc., Columbia, MD.)

9. William Claiborne, "Vials Seized by FBI in Las Vegas Are Found to Contain 'Harmless' Anthrax Vaccine*," The Washington Post*, February 22, 1998, p. A6.

10. Charles L. Mercier, Jr., "Terrorists, WMD, and the U.S. Army Reserve, *Parameters*, Vol. 28, No. 3, Autumn 1997, pp. 101-102.

11. Joint Pub 3-13pc, *Joint Doctrine for Information Operations, Preliminary Coordination,* 28 Jan 98, Glossary.

12. U.S. Department of the Army, Army Field Manual 100-6, *Information Operations*, Washington, DC: U.S. Government Printing Office, 1996, p. 5-9.

13. Fred Cohen "wrote the book" on computer viruses, through his Ph.D. research, dissertation, and various related scholarly publications. He developed a theoretical mathematical model of computer virus behavior, and used this to test various hypotheses about virus spread. Cohen's formal definition (model) does not easily translate into "human language." See Dr. Fred B. Cohen, *A Short Course on Computer Viruses, 2nd Edition*, Wiley, 1994. Credit to Nick FitzGerald, maintainer of the VIRU.S.-L/comp.virus Frequently Asked Questions, FAQ) site on the Internet.

14. *Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection, October 1997, p. 5.

15. See *Computers Under Attack: Intruders, Worms, and Viruses*, Peter J. Denning, ed., ACM Press/Addison-Wesley, 1990; *Rogue Programs: Viruses, Worms and Trojan Horses*, Lance J. Hoffman, ed., Van Nostrand Reinhold, 1990; and David Ferbrache, *A Pathology of Computer Viruses*, Springer-Verlag, 1992.

16. *Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/T-AIMD-96-92, Washington, DC: U.S. Government Accounting Office, May 22, 1996, chap. 2.

17. *Ibid*.

18. *Joint Pub 1-02*, p. 75.

19. Richard Dawkins, *The Selfish Gene*, Oxford: W.H. Freeman, 1976; and *The Extended Phenotype*, Oxford: W.H. Freeman, 1982.

20. See *To Challenge and Defeat the United States,* Thomas P. Rona and Gerald D. Godden, 1997 (unpublished, as yet) fictional manuscript, and from this author's monthly working breakfasts/lunches with Dr. Rona in 1996 and 1997.

21. George Stein, with Colonel Richard Szafranski, USAF, Retired, *U.S. Information Warfare*, Jane's Special Report, Alexandria, VA: Jane's Information Group, 1996, pp. 145-147.

22. See Colonel Robert J. Wood, *Information Engineering: The Foundation of Information Warfare*, Maxwell AFB, AL: Air War College, 1995.

23. *U.S. Information Warfare*, p. 146.

24. Brodie, *Virus of the Mind*.

25. See Stephen E. Pease, *PSYWAR: Psychological Warfare in Korea 1950-1953*, Harrisburg, PA: Stackpole Books, 1992, pp. 81, 139-142, 151-153; and Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy*, Washington, DC: Pergamon-Brassey's, 1984, pp.122-123.

26. Frank Barnett, "Reviving American PSYOP," in *Political Warfare and Psychological Operations: Rethinking the U.S. Approach*, Carnes Lord and Frank R. Barnett, eds., Washington, DC: National Defense University Press, 1989, p. 215.

27. Author's conversations with Panamanian and Guatemalan enlisted soldiers and noncommissioned officers while stationed in Latin America from 1986 to 1988.

28. Libicki, *Defending Cyberspace and Other Metaphors*, p. 6.

29. *Ibid.*, pp. 75-96.

30. Thomas P. Rona, "From Scorched Earth to Information Warfare," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds., Fairfax, VA: AFCEA International Press, 1996, p. 10.

31. Jamie F. Metzl, "Information Intervention: When Switching Channels Isn't Enough," *Foreign Affairs*, November/December 1997, p. 15.

32. As quoted in John Archibald, "Top Marine: Don't fight yesterday's wars in 2000," *Birmingham News* (Alabama), December 3, 1997, p. B1.

33. *The Annual Report on The Army After Next Project to the Chief of Staff of the Army*, July 1997, p. 14.

OUR NEW OLD ENEMIES

Ralph Peters

Our enemies of the future will be enemies out of the past. As the United States armed forces put their faith and funding behind ever more sophisticated combat systems designed to remove human contact from warfare, mankind circles back to the misbehaviors of yesteryear. Technologies come and go, but the primitive endures. The last decade of this millennium has seen genocide, ethnic cleansing, the bloody rending of states, growing religious persecution, the ascendancy of international crime, an unprecedented distribution of weaponry, and the persistence of the warrior—the man of raw and selfish violence—as a human archetype. In the 1990s, our Gulf War was the sole conventional conflict of note. Both lopsided and inconclusive, it confirmed the new military paradigm—the United States is unbeatable on a traditional battlefield—but that battlefield is of declining relevance.

We have failed to ask the most basic military question: Who is our enemy? Our ingrained response when asked such a question is to respond with the name of a country—10 years ago it was the Soviet Union, while today China is the preferred answer. We are desperate for enemies who make sense to us, who certify our choices and grant us clarity of purpose. But the age of warfare between states is waning—it may return, but it is not the preeminent military challenge of the coming decades. I believe we must ask that question, "Who is our enemy?" on a much deeper level. We must study the minds and souls of violent men, seeking to understand them on a level our civilization has avoided for 2,000 years. We can no longer blame atrocities and the will to violence on the devil, or on mistaken ideologies, or even on childhood deprivations. None of the cherished explanations suffice. In this age of technological miracles, our military needs to study mankind.

Morally, the best among us may be those who argue for disarmament. But they are mistaken. The heart of the problem is not the weapon, but the man who builds and wields it. Were we to eliminate all weapons of mass destruction, as well as every last handgun and pocketknife, the killers among us would take up wooden clubs or rocks. The will to violence is within us—it is not merely a function of the availability of tools.

Man, not space, is the last frontier. We must explore him.

It should not surprise us that religions have done a better job of locating man's desires and impulses than have secular analysts, whether Hegel, Freud or media critics. Religions handle the raw clay, and only those, which address all of man's potential shapes, survive. We are defined by the full range of our desires and behaviors, not only by those worthy of emulation. Successful religions grasp our totality (and our fears). While social orders are concerned with surface effects, religions look within. And every major religion has a prohibition against killing. There would be no need for such rules were man not a killer by nature.

In the Judeo-Christian heritage, there is a commandment believers credit directly to the writing finger of God that says, "Thou shalt not kill." Think about that. Overall, the Ten Commandments did a remarkable job of cataloging human frailty. As behavioral rules they are as valid for today's techno-civilization as they were for the dreary near-Orient of 3,000 years ago. Those prohibitions acknowledged the most destructive things that we humans are apt to do, and they warned us not to do them. The warning not to kill was the bluntest commandment.

For the moment, lay aside the concept of the Old Testament as a sacred book and consider it as a documentary of human behavior: It is drenched in violence, and its moral tenets arose in response to a violent world. It begins with the plight of two refugees—Adam and

Eve—and moves swiftly to the fratricide of their children. In book after book, we encounter massacre, genocide, ethnic cleansing, rape, plunder, kidnapping, assassination, ineradicable hatreds, and endless warfare. The fall of civilizations is reported with a merciless eye, and cities vanish with a terse comment. It sounds like the 20th century: Humanity is consistent.

Historians, however, are inconsistent. Today, we have moved away from our earlier view of civilization as a process of constant improvement, with Western civilization as man's crowning achievement. Yet, the most vociferous multiculturalists and anti-modernists, who imagine virtue for all that is foreign, still insist thoughtlessly that humankind is perfectible, if only we would take the latest scholarship on the mating habits of aborigines more seriously. I do not believe that Man has improved. There is no evidence for it. Are we better than Christ, the Buddha or Mohammed, better than Socrates, Ulug Begh, Maimonides or Saint Francis? Fashions, conveyances, medicines, communications, and the sophistication of governmental structures have all evolved. Man has not. Man is the constant. Saddam is Pharoah, and Cain will always be with us.

I have chosen religious texts and figures as examples because you know them and they resonate—not because I expect you to dial a 1-800 number with a credit card pledge. Is there a more powerful, cautionary myth for a military man than that of Cain and Abel? Throughout both Testaments, we encounter violent actors and soldiers. They face timeless moral dilemmas. Interestingly, their social validity is not questioned even in the Gospels. Although the New Testament is often ambivalent toward soldiers, the thrust of the texts is to improve rather than abolish the soldiery. It is assumed that soldiers are, however regrettably, necessary. In Luke, soldiers approach John the Baptist asking, "What shall we do?" John does not tell them to put aside their arms. Rather, he answers them, "Rob no one by violence or by false accusation, and be content with

your wages." Would that the generals and admirals involved in procurement heeded that advice today.

The Bible does not sugarcoat man's nature. Belief is not required—read it as a document and you will get a better picture of the very human enemies our soldiers will face in the next century than any work of contemporary scholarship or speculation provides. From child warriors to fanatics who revel in slaughter, our future is written in our past.

Still, if you are uneasy with the Old Testament as a catalog of human behaviors, substitute another work, The *Iliad*, that is the fountainhead of our civilization's secular literature. It begins with an argument over raping rights, proceeds through slaughter and betrayal, and has genocide as its goal. It could be about the wreckage of Yugoslavia.

In our staff and war colleges, we still read Thucydides—not for the history, but for the immediacy. Has there been another historian since the Greek twilight who matched his wonder at man's complexity and our inability to fit our desires to our capabilities?

Literature is history with the truth left in. I believe we can profit from the study of the classical texts as never before. The veneer of civilization—so recent and fragile—is being stripped from much of the world. The old problems are today's problems—and tomorrow's. If we want to know "Who is our enemy?" we must look within.

I believe that mankind is a constant in a changing world. We love the familiar, and find change hard. The conflicts in which our military will engage in the coming years will have many topical causes; at bottom, however, there will be only two: Man's nature, and the impact of change upon him.

The Muezzin and the Microchip.

Whether or not we as individuals believe in a divine being, we can recognize religion as the most supple and

consistently effective behavior modification tool available to mankind. Now if you study religions—and the soldier who does not know what his enemy believes fights blindly—you will find that virtually all of them have two myths in common: a creation myth, and the myth of a lost golden age. The need for a creation story to explain our origins is self-evident—it responds to the adult counterpart of the child who wants to know from whence his little sister came. But the myth of a lost golden age, of the white and shining temple before the fall, is directly relevant to our purpose of understanding our enemies.

We live in an age of unprecedented change—this is statistical fact. Never before has so much happened on so many levels with such breathtaking speed. Developments in a wide range of disciplines tumble over one another in a practical and psychological avalanche. Whether we speak of social structures and gender relations, medicine, communications and the utility of information, the changing nature of work and wealth, convenience and the shape of the inhabited landscape, or the sheer revolution of choice available to our citizens, our society has undergone a greater degree of intense and layered change than has any human system in history. It is a tribute to the robustness of our civilization that we have coped so well with change thus far. Other civilizations and cultures—and individuals elsewhere—are less resilient and are not coping effectively; in fact, they are decaying. And the decay of a culture is the human equivalent of the decay of atomic particles.

We live in an age when even the most adept, confident man or woman feels the earth shifting underfoot. In the parlance of strategic theorists, change is destabilizing. In the experience of the human being enduring it, change is confusing, threatening, and often hurtful. In the great scheme of things, most change turns out to be positive for most people. But it is only rarely so perceived.

Especially as we grow older, our eyes play tricks on us—we are more likely to see that which is lost than that

which is gained. How often do we hear our colleagues, friends or relatives complain about the passing of the good old days or how much better things were under the old boss (forgetting how that boss was resented during his or her tenure)?

Experience is of two kinds: that which we undergo, and that which we remember. Those "good old days" were not better. If man has not developed much, his (and certainly her) opportunities have. But we long for the certainty of that which we have known, suffered, and survived—especially when it lies at a safe distance. When I was a kid, a drugstore in my hometown displayed a poster showing a little boy lowering a bucket into a well. The print read, "Remember how sweet the water was from the old well? It was the leading cause of typhoid fever." I have never encountered a more succinct description of man's relationship to change. In our memories, we sweeten the waters of the past and erase the dirt and sickness from the myths we make of our experience.

Men fight for myths, not for truth.

Those myths of the lost golden age are most seductive in turbulent times. In the ferocity, confusion, and competition of the moment, we need to believe that things were not always so hard or so unfair, that there was a time of greater kindness and justice, when man's better qualities prevailed—and that such an epoch might return, if only we take the correct actions. Whether a radicalized mullah aching to turn back the clock to the days of the great caliphs, or a weekend militiaman in the Midwest longing for the surety of a misremembered childhood, the impulse to believe that times were better once upon a time is universal.

The experience of change and the consequent impulse to gild the past are also timeless. I wrote above that we live in an age of unprecedented change. This is true. Yet, it is also true that men and women in past ages have lived through times of then-unprecedented change. They, too, have felt the earth shake beneath their feet and heard the heavens

rumble. Accounts of the early days of the locomotive and telegraph are packed with wonder and warning. An early weapon of mass destruction, the crossbow, was outlawed in its time by secular authorities and by the Pope. Poets have always wept over the prosaic nature of their own ages, when the beauty of the past lay murdered by the practical. Can we imagine the shock at the arrival of bronze weapons felt by the people of the ancient Middle East? How the villager must have recoiled from the stench and temptation of the rising city. The first wooden cask would have excited mockery and the insistence by the old guard that wine was meant to ferment in clay pots and that was that. The potato, the most revolutionary food in modern history, terrified Europeans when it was first imported, inspiring the belief that it caused leprosy, among other diseases. The information is lost to us now, but try to imagine the shock the first laws codified by a state produced in ancient populations governed until then by custom and by fear of the supernatural. For that matter, imagine the shock a legitimate, enforced code of law would produce in Russia or Mexico today.

Given our fear of change, it is astonishing how intensely we have developed our civilizations, if not ourselves. We have changed the world—but all we have changed about ourselves are our table manners.

This fear of change and the longing for the preservation or resurrection of an old order are relevant stuff for us. Even when our enemies are not personally motivated by the fear of change, it is the fears of their neighbors that grant those enemies opportunity. Wrapping themselves in the cloak of a convenient cause, they exploit any rupture between the governing and the governed, any gulf between a prospering "progressive" elite and the stagnating ranks of believers or traditionalist masses. The men who guide the world to massacre understand the power of a call to the banner of nationalism, or an appeal to tribal supremacy, or an invitation to do some god's cleansing work with fire and sword. Demagogues capitalize on the sense of a trust

betrayed and the "evil" of the new. They are geniuses of blame. All of their failures, and the failures of all of their followers, will forever be the fault of another.

Men will fight to the death to cling to a just-bearable past rather than embrace a less certain future, no matter its potential.

In any age of great change, human beings respond by turning to religion and resuscitating tradition. In the age of science, the frightened turn to belief. Perhaps the truest of all our cliches is that "Ignorance is bliss." Men and women do not want to know. They may be pleased to learn of the misfortunes of their neighbor—television talk shows have their roots in tribal whispers—but they do not want to know that their way of life, of belief, of organizing, learning, producing, and fighting, is a non-competitive bust. The greatest impact of this information age is that it forces awareness of their inadequacy on the global masses.

At the height of the British Empire, the average imperial subject had no idea how his rulers lived. Today, the poor of the world's slums—the subjects of America's cultural and economic empire—are on to the lifestyles of the rich and famous, courtesy of television, films, video, radio, cassettes, and appalling local journalism. They do not, of course, grasp our reality. But they believe they do. The America they see is so rich and powerful it can only be predatory. It must have robbed them to grow so rich. It has no right to be so rich. And it is unjust that we should not be so rich.

The media provide instant myth. An illusion of America arrives, courtesy of lurid television serials, that is not only exaggerated in its wealth, ease, and sexuality, but that is devoid of antecedents. The world sees our wealth, but not the sufferings of our ancestors in the creation of that wealth. It is as if our riches had fallen from the skies. It is an unbearable spectacle to those who have not.

At the same time, those who watch from abroad, appetites growing, find themselves less and less able to

compete with the American juggernaut. Economic structures, the decline in the relative value of muscle power, educational inadequacies, social prohibitions, and counter-productive customs, the ineffectiveness of civil law . . . these things and more constrict the potential of other cultures to compete with the Great West—the United States and our most culturally-agile allies. Even cultures that appeared poised to break out to near-equivalence with us, such as those of Southeast Asia, hit cultural ceilings—and such ceilings are made of iron, not glass.

Most analysis of the current plight of the Asian "tigers" focuses on economic issues—but the underlying problem is cultural: the human infrastructure could not support the level of success already achieved, let alone that which was desired. The most disappointing—and worrisome—aspect of the near-collapse of Asian economies was not the financial losses but the alacrity with which the disappointed states, leaders, and people blamed foreigners for their misfortunes, when the problems were transparently homemade. They also blamed their own minorities, especially the diaspora Chinese. Already, in Indonesia, we have seen the return of ethnic pogroms. Hatred is always more satisfying than a sense of responsibility.

When nations and their underlying cultures fail to qualify in today's hyper-competitive world, they first complain. Then, if there is no turn-around, they kill. Our future enemies will be of two kinds—those who have seen their hopes disappointed, and those who have no hope. Do not worry about a successful China. Worry about a failing China.

And even a failing China is unlikely to become the threat defense contractors would have us believe. China is culturally robust. Our most frequent opponents will rise from cultures on the rocks. In our grim century, Russia and Germany grew most dangerous after their systems of cultural organization failed. Above all, this means the Islamic world will be a problem for the foreseeable future,

since it is unprepared to deal with the demands—and mandatory freedoms—of the post-modern age. Beyond that faded, failing civilization, watch out for other change-resistant cultures, from tribes and clans to states that never shook off agrarian mentalities. None of these will threaten our homes; abroad, however, they will threaten our preferred order and the extraction of the wealth that pays for our homes.

Contrary to the satisfying myths of the Left, the United States did not build its new cultural-economic empire on the backs of the world's workers and peasants. But, thanks to the information age, we will expand that empire at the expense of failing cultures. The Left understood neither the timeline nor the dynamics. And the Left still gets one huge thing wrong: the notion of American malevolence. The United States prefers prosperous markets—impoverished masses don't buy much software—but we cannot force people to be successful.

Those who fall by the wayside in global competition will have themselves, and their ancestors, to blame.

Sherman, Set The Way Back . . .

With the anti-modern tide of fundamentalism that has swept away regimes and verities over the past two decades, we have come to accept, once again, that religious belief can turn violent. Yet, when we analyze our opponents, we insist on a hard Joe Friday, "just the facts" approach that focuses on numbers, hardware, and, perhaps, a few of their leaders. We maintain a mental *cordon sanitaire* around military operations, ignoring the frightening impact of belief on our enemy's will and persistence. We accept the CNN reality of "mad mullahs" and intoxicated masses, but we do not consider belief a noteworthy factor when assessing our combat opponents. Yet, only plagues and the worst personal catastrophes excite the religious impulse in man to the extent that war does.

The interplay of religion and military violence deserves books, not just a few paragraphs. But begin with that which we know. In vague outline, we are all familiar with the Great Indian Mutiny, when the British East India Company's native levees, both Muslim and Hindu, reacted to a rumor that their new cartridges had been soiled with pig fat or beef lard by rising up and slaughtering their overlords. While any Marxist will tell you there were structural factors at play in the Sepoy Mutiny and that the cartridges were but a catalyst, the fact remains that the most savage experience of the Victorian era was the butchery of the Mutiny—first the atrocities committed against British men, women, and children, then the slaughter perpetrated against the native population by the British.

The Great Mutiny offers only a hint at the religious violence once extant in the British Empire. London's imperial history offers an interesting study for today's problems; the overwhelming impact of industry-backed regiments against native masses, the shattering of established orders, the spiritual dislocations of the defeated . . . all this is replaying around us, and will play on into the next century at fast-forward speed. Notably, Britain's most embarrassing defeats of the 19th century were dealt the empire not by other organized militaries, but by true believers—whether the ferocious holy warriors of Afghanistan or the devout Calvinist Boers. Again and again, resistance to British influence or rule rallied around a religious identity, whether following the Mahdi in the Sudan or, in our own century, struggling to recreate Israel. Our own national introduction to imperial combat involved a Chinese revivalist order, the "Fists of Righteousness," or Boxers. In the Philippines, the impassioned Muslim Moros proved a far tougher enemy for us than the conventional Spanish military.

And what of the impact of belief within armies? It is a war-movie truism that the frightened and dying turn to the chaplain, but, if we argue individual cases, we might

conclude this is evidence of desperation, not of a genuine propulsion toward belief. Yet, consider our own bloodiest conflict—the Civil War. It saw a widespread religious revival in blue ranks and gray—although as the South's condition worsened, the intensity of religious fervor in the Confederate armies grew extreme. Although it is unfashionable to say so, there is ample evidence that, for many on both sides, this was a holy war. Certainly, the hungry, ill-clothed men in the Army of Northern Virginia fought with the determination of martyrs. Stonewall Jackson entered the war a religious extremist and fought with a holy warrior's dedication. Sherman was a secular fanatic produced by an age of belief. His march from Atlanta to the sea, then northward through the Carolinas, was executed with a religious fervor, if without religious rhetoric. When we return to the sources—the letters and reports—it is clear that God was very much with both sides.

This is an ancient phenomenon. Return to the *Iliad*. Read differently and more closely this time. Don't skim the long passages detailing sacrifices or the name-dropper poetry about squabbling gods. Look at what Homer tells us about belief in the ranks. The book begins with Agamemnon's defiance of the ordained order of things—a middle finger thrust out not only at Achilles but at the gods. The Greek forces suffer for it. Plague sweeps over them. The Trojans briefly turn the tide. *And the Greeks respond in terms of their religion*. The first step is not a new battlefield strategy, it is a religious revival. Even the king must be called to order. Penitence is in. Sacrifices must involve real sacrifice. Certainly, the return of Achilles to the fight boosts morale—but the Greeks also experience a renewed sense that the gods are on their side. Meanwhile, in threatened Troy, an other-worldly fatalism takes hold, dark prophecies ring out, and Priam and his people search for an explanation of their impending fall in the will of the gods.

Of course, we do not read the *Iliad* that way. It is not our habit; we shy away from manifestations of faith, suspecting or ignoring them, or, at best, analyzing them in the

dehydrated language of the sociologist. But if we want to understand the warriors of the world, and the fury that drives them, we had better open our minds to the power of belief.

In our own Western cultural history, the fiercest military brutalities and the most savage wars were fought over faith, whether Crusades or defensive wars against Muslims, campaigns of suppression against dissenting Christians, the great religious wars of the 16th and, especially, 17th centuries, or the 20th century's world wars between our great secular religions.

Now our history is playing out in other flesh. When Indonesian rioters murder Chinese merchants, or when the Sudanese Muslims who hold power butcher and enslave the Christians in their country's south, their behavior is not inhuman. On the contrary, it is very human, indeed.

Beware the enemy motivated by supernatural convictions or great moral schemes. Even when he is less skilled and ill equipped, his fervor may simply wear you down. Our military posture could not be more skewed. We build two-billion-dollar bombers, but we cannot cope with barehanded belief.

The Shaman and the Gangster.

If the intoxicated believer is one very dangerous extreme in the range of our enemies, the other is the man utterly free of belief, or fear of the law, or civilizing custom. When you encounter them together—the saint and the cynic in league—you have the most dangerous combination on earth. Charismatics and opportunists are a dynamic match, as many a successful televangelist instructs us. You see it in a sloppy fashion with Saddam Hussein and his belated attention to Islam, but also in the alliance between Kremlin bandits and the Orthodox Church.

From Algeria's religious terrorists to politicians anywhere who align themselves with religious movements

whose convictions they privately do not share, it is often difficult for us to determine where the prophet ends and the profiteer begins, how much is about faith and how much about grabbing power. In such cases, we tend to err on the side of cynicism, preferring to impute base motives to our enemies (even as we imagine that those enemies are somehow redeemable). But slighting either side of the equation, the human potential for cynicism or for belief, brings us only half-answers. In conflict, the saint and the cynic can complete each other without consciously understanding why their alliance works so well—together they combine the qualities of the cobra and the chameleon.

The most difficult thing for Americans in (and out of) uniform to face may be that even the most powerful military can, at most, briefly alter outward behaviors. We subdue belief only by killing the believer. The opportunist will bow to the threat of lethal power—until you turn your back. But no display of might will change the essence either of the man driven by God, or of the man driven by greed.

We have entered another age when empires begin to learn their limits. While our empire has—and will maintain—informational dominance, we cannot dictate which information will be accepted and acted upon by foreign populations. We can flood them with our culture, shock them into doubt, sell them our wares—but we cannot make them behave as we would like . . . unless we are willing to commit brutalities on a scale that would destroy our own myth of ourselves.

Certainly, if sufficiently provoked, we are capable of killing plentifully and with enthusiasm. But such events are exceptional. In their balance and wisdom, the American people will fight genuine enemies, but they would not now countenance the slaughter of foreign populations over distant misbehaviors. The mark of our civilization's greatness is a very simple but very rare one: at this point in our social development, we would rather do good than evil,

so long as it doesn't cost too much. It is a surprisingly rare quality.

Elsewhere, there is less interest in the inviolability of the individual or of his society, if it is foreign and subscribes to a different creed. We face enemies whose sole motivation to refrain from killing is the fear of being killed. Nothing else moves them. It is difficult for Americans, with our lack of historical knowledge and our fuzzy notion of the validity of all cultures, to grasp the richness of hatred in this world. For all of our alarm over crime, most Americans live in an astonishingly safe environment. We are not threatened, and we behave cooperatively and corporately. But our safety is both the result of and contributor to our insularity. We lead sheltered lives. And we imagine that the rest of the world is just like us, only less privileged.

But the rest of the world is not like us. For all of our lingering prejudices, we have done a remarkable job of subduing our hatreds. Perhaps it is only the effect of wealth bounded by law, but we are a powerful exception to history. We are indescribably fortunate—but our good fortune has lulled us into our primary military and diplomatic weakness: we do not understand the delicious appeal of hatred.

We cannot understand how Serbs, Croats and Bosnian Muslims could do that to each other. We cannot understand how Hutus and Tutsis could do that to each other. We do not understand how the Chinese could do that to the Tibetans. We do not understand how the Armenians and Azeris could do that to each other. We do not understand how the tribes of Sierra Leone or Liberia could do that to each other. We do not understand how India's Hindus and Muslims could do that to each other. We do not understand how the Russians and Chechens could do that to each other. We do not understand how Haitians, Somalis, Colombians, Mexicans, Indonesians, Sri Lankans, Congolese, Burundians, or Irish could do that to each other. . . .

Over the years, I have written about "warriors," the non-soldiers we encounter and fight, from guerrillas to narco-traffickers. In the past I stressed the importance of recognizing five types of warriors: the scum of the earth, the average Joe who is drawn into the conflict as it drags on, demobilized military men, opportunists, and true believers. Now I worry about only two of these sources of conflict—the opportunists and the believers, the gangsters and the Godly, the men unrestrained by morals and those whose iron morality is implacable. They are the centers of gravity. The others are swept along by the tide.

Man, the Killer.

Of all the notions I have advanced over the years, only one has met with consistent revulsion and rejection—the statement that men like to kill. I do not believe that all men like to kill. At the extreme, there are those saintly beings who would take their own lives before taking the life of another. The average man will kill if compelled to, in uniform in a war, or in self-defense, but has no evident taste for it. Men react differently to the experience of killing. Some are traumatized. Others simply move on with their lives. But there is at least a minority of human beings—mostly male—who enjoy killing. That minority may be small—but it does not take many enthusiastic killers to trigger the destruction of a fragile society. Revolutions, pogroms, genocides, and civil wars are not made by majorities, but by minorities with the acquiescence of the majority. The majority may gloat, or loot, but the killing minority drives history.

Violence is addictive. Police know this. That's where the phrase "the usual suspects" comes from. In our society, the overwhelming majority of violent acts are committed by repeat offenders. Statistics would make us a violent nation; in fact, we are a peaceable people until aroused. The numbers are skewed because we have failed to deter recidivists. Spouse- and child-abusers do not do it

once—they repeat. Sex offenders—and sex crimes are all crimes of violence—are notorious repeat offenders. Most barroom brawls are begun by the same old troublemakers. Even in combat, when mortal violence is legal, most enemy combatants killed in close fighting appear to be killed by a small number of "high performers" in our ranks. Throughout history, many a combat hero has had difficulty adjusting to peace.

We reject the evidence of the human enthusiasm for violence because it troubles us and undercuts the image we have created of perfectible Man. But violence has an undeniable appeal. Certainly for the otherwise disenfranchised, it is the only response left. Perhaps the psychologists are right that much violence is a cry for help. But what both of those arguments really say is that violence, however motivated, is gratifying and empowering.

Religions and civilizations may be seen as attempts to discipline mankind, to trim our worst excesses. Traditionally, religions and civilizations acknowledged mankind's propensity for violence and imposed appropriate strictures. Certainly, no religion or civilization has believed it could ignore violent behavior as peripheral. Yet, our contemporary American approach is to treat violence as an aberration, the product of a terrible misunderstanding. It is the mentality of the born victim, of the abused spouse who believes every weeping apology, of the social worker who believes in the mass murderer's rehabilitation. Our willful denial of the full spectrum of man's nature, from the sublime to the beastly, is a privilege of our wealth. It is not a privilege that will be extended to our soldiers.

Look at the wreckage of this decade. Can we pretend that the massacre of half a million Rwandan Tutsis by their neighbors was carried out as a laborious chore? On the contrary, reports from the scene describe murderers intoxicated by their deeds. When we consider the ingenious cruelties perpetrated daily in Algeria, can we believe that the killers are forced to commit those atrocities against

their inclinations? Will we pretend that the dead of Srebrenica were the victims of reluctant hands?

A meaningful sense of humanity demands that we ask hard questions about the nature of man. Military effectiveness in the coming decades will make the same demands. It will be terribly difficult for us. Our uniquely noble elevation of the individual's worth is ill-suited to a world in which our opponents regard the masses that follow them as surplus capital.

The American Myth of Peace.

A corollary to the universal myth of a lost golden age is the recurring myth of the peaceable kingdom, where the lion lies down with the lamb and the spear is broken in two. This has long been a powerful myth in the American ethos, carried from Europe by the first colonists who sailed for New England. Especially in those northern colonies, many of the early settlers belonged to dissident Protestant sects out to replicate the kingdom of God on earth. Many were pacifists—at least among their brethren—or had strong pacifistic inclinations. They had been oppressed and, no matter that they would become oppressors in their time, their experiences had condensed their vision of a just, ideal world to diamond hardness.

Our founding fathers and mothers fled Europe's dynastic struggles convinced that such wars, and by extension all wars, were ungodly. Later, they fought the Indians, then the French, then the British, then their southern neighbors, then much of the world. But they never accepted war as in the natural order of things. War was a terrible, unnatural misfortune, perpetrated by despots and madmen, or spawned by injustice. But it was not a core human endeavor.

From that heritage we Americans have developed our ahistorical belief that all men want peace, that all conflict can be resolved through compromise and understanding. It

leads to the diplomatic equivalent of Sunday-night snake handling—faith in the power of negotiations to allay hatred. Because we are privileged and reasonably content with our corner of the planet, we find peace desirable. There is nothing wrong with this. The problem arises when we assume that all other men, no matter how discontented, jealous, disenfranchised, and insulted, want peace as well. Our faith in man is, truly, a blind faith.

Many human beings have no stake in peace. They draw no advantage from the status quo. We even see this is our own fortunate country. A disproportionate share of crime is committed by those with the least stake in society—the excluded and marginalized with little or nothing to lose. In this age of accelerating change, we, too, suffer from extreme fundamentalism concentrated at the lower end of the social spectrum (though not at the bottom among the drug-wrecked Lumpenproletariat). Consider the crimes that trouble us most. Gang crime occurs between those with the least to gain or lose from the social order the rest of us cherish. The Oklahoma City bombing was the work of a man who felt rejected by the society around him, who felt wronged. The repeated bombings of abortion clinics consistently prove to be the work of low-skilled males who have turned to aggressive religious beliefs in which tolerance is intolerable. Dangerous true believers and violent opportunists are very much with us in our own homeland.

We are, however, better positioned to control their excesses. Neither right-wing militias nor extreme fundamentalists are going to take over our country in the foreseeable future. But much of the world is less fortunate. Where there is less opportunity (sometimes none) and the existing, comforting order shrivels, human beings want validation and revenge. They cannot accept that their accustomed way of life is failing and that they are failing individually because of the behaviors to which their culture has conditioned them. They want someone to blame, and then they want revenge on that someone. A leader, secular

or religious, has only to preach the gospel of foreign devils and dark conspiracies—to absolve his listeners of responsibility for their own failures—and he will find a willing audience. Humans do not want change. They want their customs validated. They want more material possessions, but they do not want to alter their accustomed patterns of behavior to get those things. This is as true in America's inner cities as it is in the slums of Karachi or Cairo.

Again, many human beings thrive on disorder. When the civil war ends, the party is over. Many of the difficulties in Bosnia today stem from warriors who built thriving black market and criminal networks during the fighting and do not want to let go of them. Often, those who do the bulk of the fighting are men ill equipped to prosper in peace. The gun is their professional tool. When they grow convinced by, or are at least cloaked in, nationalist or fundamentalist religious beliefs, they are vulnerable only to greater force. In Russia, much of the citizenry longs for the rule of law—even the harsh law of the past. But those who have enriched themselves during Russia's new "time of troubles" like the system just the way it is; it is difficult to convince a prospering gangster that the rule of law will work to his advantage. Around the world, from Uganda to Abkhazia, it is difficult to persuade those whose only successes in life have come from the gun in their hand that they should hand over that gun. Being a warlord, or just the warlord's retainer, is a far more attractive prospect than digging a ditch for a living—or, worse, failing to find work as a ditchdigger.

We profit from peace. Our opponents profit from conflict. It is as fundamental a mismatch as the one between our forces and theirs. When they try to play by our rules, whether in the military or economic sphere, we demolish them. When, however, we are forced to play by their rules, especially during military interventions, the playing field is not only leveled—it often tilts their way.

When we drive the warriors into a corner or defeat them, they will agree to anything. When our attention is elsewhere, they will break the agreement. Their behavior, natural to them, is unthinkable to us. And then they massacre.

We pride ourselves on our rationality, while avoiding reality. If we are to function effectively as diplomats and soldiers, we need to turn a dispassionate eye on mankind. We need to study the behavior of the individual and the mass, and to do it without stricture. We cherish the fiction that technology will be the answer to all our dilemmas. But our enemies know that flesh and blood form the irresistible answer to our technologies.

Troy and Jerusalem.

Another cliche with a core of truth is that Americans are the new Romans, proprietors of a (near-) universal empire based upon engineering and codification. Certainly, we guard the walls of our civilization against new barbarians. But the mundane parallels are more intriguing. First, even when the Romans behaved cruelly at the height of empire, it was a measured policy. Second, their military was tiny in proportion to the range of their empire, and their legions, while rarely defeated, were often astonished by the savagery of their opponents. Third, the Romans so cherished their civilized image of themselves that it blinded them to barbarian strengths.

Fanatics brought Rome down. We associate the fall of Rome with Alaric and the Visigoths and a jumble of other warrior peoples who swept in from the north for long weekends (as German tourists do today). But Rome's decline was slow, and the empire rotted from within. Romans loved the law—even under the worst emperors, the rule of law never disappeared entirely—and they grew convinced that peace was the natural order of things. Their judges sought equity and order, and their legalisms crippled them.

Let us return to our beginning and consider the New Testament. Contrary to the Christian creed, the historical figure of Jesus does not appear to have "suffered under Pontius Pilate." On the contrary, Pilate the Roman did not understand the case before him and was not certain it fell within his purview. He was baffled and annoyed by the local squabbles, failed to appreciate the social and religious complexities involved, and just wanted the problem to go away. He was the classic representative of empire. We can almost smell the heat of the day and imagine the Roman's impatience with his translator. When arbitration failed, Pilate "washed his hands" of the prisoner's fate, more diplomat than soldier. Pilate was a symbol of weakening Rome and growing Roman self-doubt. He served at Rome's apogee, yet the cancer was already there. His descendents, preferring debate to decision, would be no match for the fanatics who could kill the sober and the just without blinking. Pilate stuck to the letter of the law, and the law damned him.

As empires fall—and I am not suggesting that our own empire will fall for a long time—the people of the empire return to religion. Christianity, a liberating mystery religion of the lower classes, had to struggle during the heyday of the Roman empire. But when the decline became impossible to deny, the new religion, with its revolutionary rhetoric, prospered. In prospering, it further accelerated the decline of the old order. The repressions were too little too late.

The Romans were chronically late to respond to challenges in the age of the lesser caesars. The destruction of Solomon's Temple in Jerusalem and the suppression of the Jewish kingdom was not a sign of remaining imperial strength, but of weakness, frustration, and decline. In its confident years, the Roman Empire had been absorptive and tolerant. For centuries, these qualities lent strength and co-opted new subjects—but ultimately core identities and commitments to the Roman idea were fatally diluted. It was those who refused to be absorbed and who rejected

toleration, from the brute German tribes to the true believers from the eastern provinces, who outlasted the greatest empire the earth knew until our own century.

We can measure historical climates by reading the growth bands of a tree stump. We can measure the climate of a culture by noting its religious revivals or the advent of a new religion—each marks a time of great stress on the society. In 1998, we are living in the most passionately religious age in centuries. The future looks ferocious.

Leaving aside the threat from weapons of mass destruction, however, the United States appears invulnerable for the foreseeable future. Terrorists might annoy us, but we will triumph. We will, ultimately, find the strength of will to do what must be done. The problems raised in this essay affect the average, prosperous American citizen little, if at all. But it is the soldiers of our new empire, the men and women who serve in our expeditionary forces and deploy to subdue enemies we refuse to understand, who will pay the cost of our willful ignorance. They will still win, when allowed to do so. But more of them will suffer and die for lowered returns because of our stubborn unwillingness to face the complexity of mankind.

Come back now to Troy. Read that great poem one more time, without the prejudices we have learned. You will find that the triumphant Greeks were the devious, the barbarous, and the murderous. The Trojans were the urban, civilized, and tolerant. Troy stood for learning, piety, and decency. Its mistake was to humiliate implacable barbarians, without the will to destroy them. The Trojans fought to be left alone in their comfortable world. The Greeks fought for revenge, spoils, and the pleasure of slaughter. The Greeks won. Ulysses, who finally inveigled a way through the city gates, was the first great Balkan warlord. Murdered King Priam was a decent man who watched the war from behind his walls and had to beg for the return of his son's mangled body. He was presidential in his dignity.

We are not Trojans. We are far mightier. We rule the skies and seas, and possess the power to rule the land when we are sufficiently aroused. But we have not learned to understand, much less rule, minds and hearts and souls. The only moral we need to cull from the *Iliad* is that it is foolish to underestimate the guile and determination of the killers from the other shore.

PART III: STATE-ON-STATE APPROACHES

INTRODUCTION

Lloyd J. Matthews

In Part III—State-on-State Approaches, we move from particular asymmetric threats to U.S. security to particular countries that might pose such threats. Strategic analysis remains incomplete if it merely dissects how we can be hurt or defeated, failing to connect such vulnerability to concrete capabilities of actual or potential enemies from this world.

In "How We Will Lose the War With Russia: A Critique of U.S. Military Strategy," Dr. Stephen J. Blank offers the thesis that in a war with Russia we could well suffer politico-strategic defeat despite achieving decisive operational success. At the outset, Dr. Blank notes that it is hard to construct a rational definition of victory that does not entail the destruction of Russian nuclear and/or conventional capability, the collapse of its government, or the occupation of Russian territory. Yet, would we want any of these things to happen? Would they bring us a better peace? Dr. Blank goes on to point out that any one element of this notion of victory implies total war, which itself becomes unthinkable given Russia's still formidable nuclear arsenal.

How could we find ourselves in this kettle of fish? Ironically, according to Dr. Blank, it could be the result of our own misguided declaratory policies, aided and abetted by our arrogance regarding the oft-sung epic prowess of the Army After Next.

By advertising our capability and intention to wage massively destructive, simultaneous, multi-level war throughout the depth of the enemy's homeland and to decapitate his government by destroying all nodes of command, control, and communications, we effectively threaten a war that from the enemy's perspective is total.

Such a perception opens the door to desperate acts of preemption or retaliation by the enemy, employing nuclear and other weapons of mass destruction. We thus fall victim to our own hoopla in behalf of the vaunted technological and informational superiority produced by the Revolution in Military Affairs.

The RMA and its important derivative, information warfare, doubtlessly do confer upon the United States significant asymmetric advantages over Russia at the operational level of war. But rather than continuing to gloat publicly over these advantages, in the process propounding a dangerously aggressive strategic doctrine for employment, U.S. thinkers must, in Dr. Blank's view, devote harder thought to the limitations of new weapon systems and particularly to the second- and third-order effects of the doctrine for employing them, and then align that doctrine with America's true politico-strategic aims and interests.

In "Regional State Competitors: The Case of Iraq," Dr. Stephen C. Pelletiere undertakes to demonstrate that in the Gulf crisis of February 1998, featuring an asymmetrical test of power between Iraq and the United States, the weaker power won. In this sobering study, perfectly suited to a conference on asymmetrics, we learn, or re-learn, that victory doesn't always go to the party with the bigger battalions.

It is true that Iraq did finally accede to the resumption of biological-chemical weapons inspections, but it did so only after having stalled long enough to perform any necessary sanitization of suspect storage and manufacturing sites, and after isolating the United States from its 1991 Gulf War coalition allies. By cleverly playing upon Arab resentment of the U.S. double standard in dealings with Iraq vis-à-vis Israel, by exploiting European resentment of U.S. attempts to infringe economic ties with Iran, and by fueling domestic opposition to threatened attacks on Iraq within the United States itself, Saddam Hussein greatly weakened his

superpower enemy in any future resumption of the crisis and took a giant step toward accomplishing his goals of ending the United Nations inspections and having the economic sanctions lifted.

Lacking solidarity with its coalition partners, lacking consensus on the home front, and lacking a broadly felt sense of threat from Iraq itself, the United States would be best advised, in Dr. Pelletiere's estimation, to avoid another confrontation with Iraq and re-think its present policy of "dual containment" (isolation) of Iraq and Iran.

In "Beyond Russia and China: A Survey of Threats to U.S. Security from Lesser States," Dr. Kori N. Schake, after taking note of the supposition that a major peer competitor of the United States is unlikely to emerge within the next 15 years, sets out to discover which if any less-than-peer states (excluding Russia and China) might pose a threat in the interim.

The three "usual suspects," North Korea, Iran, and Iraq, are examined initially and found to be increasingly unlikely as credible opponents—North Korea out of abject economic weakness, Iran because of its moderating internal political environment, and Iraq owing to the continued marginality of its armed forces.

There are, however, six "nightmare scenarios," unlikely but possible, that in Dr. Schake's view could materialize to threaten U.S. security or interests: (1) anti-U.S. coalitions; (2) violent emergence of new states based upon ethnic consolidation; (3) adverse change of political orientation among existing U.S. allies; (4) political/psychological manipulations by enemy states to constrain application of U.S. force; (5) RMA-induced incompatibilities between the armed forces of the United States and those of its allies; and (6) criminalization of governments. With regard to the latter, the rise to power of criminal regimes in either Russia (with its nuclear arsenal) or Mexico (with the 2000-mile Mexican-U.S. border) would pose a particularly grave threat to U.S. security.

While Dr. Schake makes no claim that the United States could control or even materially influence all emergent scenarios antithetical to American interests, she does make the point that adequate vigilance abetted by traditional diplomatic-military tools could make America's task manageable in most cases.

Glancing back to Part I on asymmetric warfare as practiced in ages past and present, we recall one cardinal axiom: *A superior level of scientific and technological advancement along with the weaponry that goes with it does not necessarily translate to victory in war. Victory goes rather to the side that musters in its behalf a decisive share of the total universe of factors affecting man's will and ability to coerce his fellow man*.

In Part II addressing generic threats to American security over the next 20-25 years, we learned that those threats can take new and unexpected forms. Enemies unable to outmatch us on our terms will exert great ingenuity and resourcefulness to outmatch us on their terms, particularly in areas where we are too negligent, too complacent, or too proud to attend. Part III teaches much the same lesson, reminding us additionally that relatively backward states taken for granted can rise up to smite us when conditions are right. America the technological and information behemoth beware.

HOW WE WILL LOSE THE NEXT WAR WITH RUSSIA: A CRITIQUE OF U.S. MILITARY STRATEGY

Stephen J. Blank

Introduction.

The ignominious fiasco of our campaign against Iraq showed that our strategy was deficient or had gone on holiday. We have clearly forgotten that war remains the continuation of politics by other means which are employed to obtain a supposedly better peace. Hence the strategy that cannot materialize political goals either through war or peaceful means is defective. Our Iraqi experience shows that we cling to failed strategies and ways of thought, that we still see war as being distinct from politics and military operations as distinct from strategy.

These defects apply with particular force to a (hopefully) purely hypothetical war with Russia or any potential peer competitor. Indeed, such a scenario immediately raises the question of devising a rational definition of victory. A victory in a war with Russia must mean either the destruction of Russian nuclear and/or conventional capability, the collapse of its government, or the occupation of Russian territory. Any of these definitions of victory must entail a total war which should be ruled out due to Russia's nuclear arsenal. But even if we won without going nuclear, we would have ultimately won nothing and fought a war with little or no strategic rationale. However, that consideration does not necessarily prevent the unthinkable from becoming real. Indeed, our infatuation with technological revolutions in warfare suggests that we still seek to wage limited high-tech conventional war without fully grasping that doing so against major rivals entails a total war. Army strategy, for instance, proclaims that it will be satisfied with nothing less than decisive victory, but if victory cannot be

plausibly defined then what happens?[1] Our strategy does not know where it is going. Thus the inherent difficulty of defining a true strategic victory in what would almost inevitably be a total war for our enemy suffices to call our strategy into question.

That strategy rests on the oft-cited formulation of "leveraging" technological superiority and converting it into operational and strategic superiority. However, the revolution in military affairs (RMA) and our superiority in information warfare (IW) are not surrogates for strategy and do not eliminate the need for it. Indeed, the wonder weapons we possess cannot deprive Iraq of a weapons of mass destruction (WMD) capability, locate its sources, or overcome the shortfall in intelligence regarding the location of Iraqi WMD assets and capabilities. The confident prophecies that the battlefield will soon be subject to our global reconnaissance technologies—meaning that if you move, you die—are premature.[2]

Therefore we must locate the deficiencies in our own strategy, which can cause strategic defeat or failure (against Russia or comparable rivals) even if we win an overwhelming battlefield victory. Moscow is already preparing materially and doctrinally for contemporary and future war. While Russia probably cannot acquire all the necessary skills and integrate all the aspects of modern platforms to create RMA and IW capable forces, it continues to upgrade its forces' capabilities towards that end. We can expect Russia to continue to explore new capabilities and ideas since it feels it must resist U.S. power.[3]

Problems of U.S. Strategy.

First of all, to attain victory, however we define that term, we must overcome our own ingrained tendencies to chauvinism, insularity, and ethnocentrism in military affairs.[4] Otherwise those qualities, born of past success, will handicap us in any contest with foreign states, political or

military. We ignore foreign countries' ideas and situations at our peril and risk losing victory at the strategic level.

For instance, it is commonly accepted that current concepts of the RMA and of IW constitute a uniquely American doctrine of war. The next century is confidently expected to be an American one where everyone follows our example. Everyone must follow in our wake or fall apart.[5] And that fact gives us a lasting information edge. This state boosterism is often accompanied by an equally triumphalist and pervasive service boosterism that obscures more than it enlightens. Indeed, some Air Force writers regard the current dominance of U.S. air power as revealing an almost mystical relationship between a supposedly more democratic form of military power and the world's leading democracy.[6] But both service and national ethnocentrism are grievously misplaced.

Indeed, the very concept of the RMA originated in Soviet military thought as a response to the advent of nuclear weapons and the dawn of the cybernetic age.[7] Soviet writers sought to use conventional arms to obtain a decisive strategic result in Europe and, to a lesser degree, in Northeast Asia.[8] They sought to achieve victory and avoid nuclear war through deterrence or parity, or by destroying our strategic weapons in Europe in the first hours of the offensive. They also contemplated their own first strike attack on our strategic forces but could never figure out how to avoid a subsequent unwinnable nuclear war.[9] But both they and we were essentially driven by the search for usable military power.

In the 1980s we appropriated the term RMA and other Soviet operational concepts like Airland Battle and Follow on Forces Attack. As the Soviet regime fell apart in the 1990s, we conducted a textbook Soviet-style offensive in the Gulf in 1991 as the Soviet Chief of the General Staff claimed to U.S. visitors.[10] Thus our paradigm was born in Moscow although Moscow could not realize its theoretical innovations in practice.

Nevertheless our current thinking about war, derived from Operation DESERT STORM, could lead us into failure to understand modern warfare and strategy. The Iraqi crisis of February 1998 suggests that this failure may not be far off. Indeed, it is all too apparent that our strategy essentially consists of a mechanical repetition of preparing to fight the last war again and again. We have failed to translate our earlier battlefield victory against Iraq into a lasting status quo, where we no longer must revisit the scene and use force again under much worse political conditions. If we should fall into conflict with Russia, we will not have the luxury of revisiting the theater 7 years later to try to rectify our mistakes. Nor do we have the luxury of the leisurely buildup of forces in the theater that characterized DESERT STORM.

Given the prevailing and all-encompassing sense of threat in Russian military writing, Moscow would likely view a war with us as an unlimited or total war. Whether we won by destroying conventional forces and escaping nuclear conflict, or somehow destroyed or neutralized Russia's nuclear capabilities, or even occupied parts or all of Russia, there is no way any Russian government could survive. That government would disappear or at least lose territory. And we, like the foreign occupiers in 1918, would be forced to occupy and patrol vast areas of a nuclearized former Soviet Union—clearly an absurd strategic result. Yet once we make our central target and center of gravity the stability of the enemy's government, as our strategy and doctrine do, we have made that war a total war for our enemy. Almost without realizing it, we have converted our operational template, believing it to be one of limited war, into an asymmetric total war for our enemy. This strategic nonchalance inevitably has profound and far-reaching results. To embark upon it means gambling on revolutionary transformations beyond our control, imagination, and understanding.

Indeed this unthinking jeopardizing of our strategic goals through an asymmetric war almost suffices to

guarantee strategic failure since nobody can give a plausible definition of victory. Where the proper limits of operations cannot be determined or imposed, the end result is invariably chaos, revolution, and defeat, as Bismarck predicted in 1887-88 and as came true in Germany's "victory" over Russia in the First World War.[11]

Our quest for military victory, based on our economy and modern technology's astonishingly innovative capabilities, pushed us to pursue qualitative superiority against the massive Soviet armies. This "offset strategy," first developed by Secretary of Defense Harold Brown in the 1970's and then carried forward by the Reagan and Bush Administrations, aimed not only to give U.S. forces qualitative superiority, but also the capability to defeat Soviet forces by innovative and borrowed operational and strategic concepts, including global economic and propaganda warfare.[12] These forms of warfare must be listed in any objective account of U.S. strategy to use technology and telecommunications to attain high-level strategic objectives, including the destabilization of enemy regimes.

However, whether intended or not, this strategy also provided our government and armed forces the means to achieve strategic objectives that related to more domestic, parochial concerns.The RMA and IW, at least in theory, provide opportunities to wage war rapidly at great distance by achieving air and electronic superiority as a leveraging force, sustain minimal casualties in order to overcome domestic opposition, avoid protracted war at all costs, replace the politically costly system of conscription and its associated manpower costs with technology to make up the increasing shortfall between our growing responsibilities and declining defense budgets, and constrain the media's ability to portray the war other than as the generals want it portrayed.[13] In other words, the RMA and IW supposedly enable us to overcome what many military men believed were the reasons for our loss in Vietnam and also to revolutionize warfare to our advantage.

Adherents of the RMA proclaim that it leads to a new paradigm of "distance warfare" or "parallel warfare" because it strikes at enemy targets all at once. It is a war dominated by long-range strike platforms operated by fewer soldiers, using state-of-the-art sensors, precision-guided weapons, etc.[14] New forms of war also let us overcome the dilemma of sequential operations. By linking strike and reconnaissance capabilities and platforms in real time so that forces can effect decisive strategic outcomes in the initial operation and collapse together the strategic, operational, and tactical levels of war, we can convert formerly sequential and interrupted operations into one decisive, rapid, continuous joint operation. This decisive operation would mount a combined, joint weapons and electronic attack on classic military targets as well as the enemy's command-control-communications-computers-surveillance-reconnaissance (C4ISR) capabilities. The latter constitutes the enemy's true center of gravity. The notion that we would successfully target the enemy's ability to know what is happening and lead its troops has been "deified" as doctrine, at least in the Air Force.[15] In the first strike alone, our technological and informational superiority would destroy the enemy's capability to command and control his troops and know what is happening. We would have effectively decapitated the enemy and could finish off the disconnected pieces of his forces in an uninterrupted operation.

Such warfare means that the first operation becomes the only one **if and only if it is successful**. No longer are there a series of sequential operations in time and space. Rather one large uninterrupted operation of devastating and unremitting force occurs quickly. There, the decisive edge goes to whoever attains technological superiority because he can control the ether, degrade the enemy's information structures and capacities, and thus nullify enemy platforms' strike capability and decision-making systems. Technological superiority can be converted into lasting strategic superiority, mainly by aerial, missile, and

electronic attack (or by the mobility and maneuver of multiple fires from different distances). The great value of the new technologies and weapons is their ability to leverage time, today's preeminent scarce factor. By mastering time, we will master our enemies.[16] And we can collapse distinctions between front and rear. The entire enemy territory becomes the theater of war. Informational nodes and C4I throughout the depths of this territory may be even more important strategic targets than are the armed forces opposing us.

Allegedly we can also destroy enemy capability with much less lethality and loss of life on both sides due to our superiority in technology and informatics. Our superiority is taken for granted, as is the supposition that we can exploit those advantages to obtain a decisive and quick victory on the battlefield, and destroying the enemy's will and capability to fight.[17] Thus information capability and superiority are vital to all our operations and activities. Information superiority confers upon us a capacity for dominant mobility, precision engagement, the capacity to deprive the enemy of knowledge about his situation through our dominant battlespace awareness, and lets us conduct focused logistics. At the same time, we can fully protect all of our assets against the enemy's attack by getting in the first blow and attain "full dimension protection." Such operations also allow us to map virtually the enemy's entire battlefield, making it completely transparent to us while our terrain remains opaque to him.[18]

Finally, by making tactical operations pay off at the operational and strategic level and eliminating the need for sequential operations by striking at the heart of the enemy in a single massive, joint, and coordinated operation, we can negate or greatly reduce friction in war. Our knowledge will be perfect or as close as possible to that state depending on which analyst you read.[19] But the enemy's knowledge will not be, and we can thus have dominant battlespace knowledge. The whole point of the operation is at least to create a decisive imbalance in the amount of friction and fog

that redounds to our advantage and can then be converted into a lasting strategic advantage. All these emblems of our technological superiority, taken together and thus multiplied in effectiveness, will confer not just operational superiority, but a lasting politico-strategic superiority and hegemony.[20]

This is not only because our superiority will remain unchallenged, but because our superior strengths will both deter and win wars. Even though conventional deterrence has been flawed in this century, to the extent that it can succeed it can best be accomplished with U.S. forces configured for deterring and winning regional or theater conventional wars.[21] But it does not end there. We are also building our military forces to become a generic military force that can use dominant maneuver, precision engagement, full protection of our assets, dominant battlespace awareness, and focused logistics, backed up by informational, technological, and weapons superiority, to win and dominate across the full spectrum of war. This spectrum includes humanitarian interventions, peace operations of all kinds, ethnic and civil wars, etc. all the way up to theater conventional, and perhaps even multi-theater war.[22] Our capabilities will be universally applicable across that spectrum.

Leveraged air power, long-distance strikes, and C4I platforms in general have become the weapons of choice to attain strategic objectives and open the path for the harmonious joint interaction of all other forces. Then they can achieve their tactical, operational, and strategic goals at reduced cost and time, and with reduced friction and fog as well. Hence, success in achieving these goals critically depends on our ability to achieve preemptive or pre-combat power projection so that we can become the decisive factor on the scene even from afar. Alternatively, our forward presence should allow us to deploy as rapidly as possible to a threatened area and resist the enemy as far forward as possible. Of course, without that forward presence or

welcoming environment for our power projection, the notion of a brief war flies out the window.

Thus we are subject to an endless race to maintain technological superiority, realize the unmatched capabilities now lying at hand, and preserve our lead over all competitors. We are also developing or at least talking about a capacity for controlling what both the domestic and the foreign media can see and hear of the war and what they present to their audiences.

The combined effects of our military technology and our informational and telecommunications industry's capabilities allow and almost mandate global strike capabilities in peacetime as well as war. These strike capabilities especially pertain to information strikes against enemy media, computers, and communication facilities that can degrade enemy awareness and knowledge even before an actual military first strike. We can strike at the enemy's front, middle, and rear at all times and obtain a real-time capability to know what is happening due to those strikes.

Accordingly, given the growing global capability to wage IW or counter IW attacks on media and computer networks, the distinction between peace and war in IW is eroding along with notions of rear and front. This capability, along with the stated intent to use it, will create a preemptive race to get in the first strike even in peacetime. But since this technology is available at low-cost to other entrants into the strategy sweepstakes, we are also uniquely vulnerable to all kinds of adversaries who are themselves conducting IW or counter-communications warfare against us.

Admittedly this picture simplifies a great many issues in the discussion of future war, but it does not caricature them. It captures the essence of the promise of future high-tech and information operations and the goals we have charted for conducting such operations. But such warfare has political, i.e., strategic, implications that are not fully discussed in our writings.

For instance, just as critical elements of IW and the RMA's operational side are the determination and the means to attack the enemy's understanding of reality, so too is this form of war uniquely well-suited to manipulate domestic opinion both here and abroad. John J. Fialka writes that the U.S. military has long been capable of secretly taking over an enemy's airwaves. Our flying television or radio studios can overcome a station's signal by a more powerful one, decisively affecting the information available to key targets. And new technologies like morphing only enhance our weapons capability to show our enemies that "truth is a very powerful weapon."[23] As many observers note, we initially saw the superweapons of DESERT STORM, not their grim effects. But once the highway of death flashed on TV screens, the images decisively altered our operational and strategic goals.[24] Foreign observers also have charged that we can devise a capability to take over a country's media (e.g., Cuba) without necessarily firing a shot.[25] This capability to strike at the opinion-forming processes of a country and government extends the war so that an enemy itself becomes a theater of war, and its media and government can become the center of the war's gravity. By this process, we again immediately make it a total war for the enemy state, with unfathomable consequences for our own forces and government. This increasingly global capability can easily be turned against us, making our own media and government the center of enemy gravity.

Future War and the Shortcomings of Our Theories.

The 1997 National Military Strategy recognizes that enemies, in this hypothetical case Russia, may strike at us using asymmetric means, WMD, unconventional war, or an adaptation of our own techniques and weapons against us.We may expect that Russia will employ all of these forms of asymmetric threat against us at the same time. We should not assume that such combined forms of warfare are mutually exclusive. The partisan warfare on the Eastern

front in 1941-45, and in France before and during the Normandy invasion, and the guerrilla war in Vietnam show how unconventional and large-scale conventional war can be combined by a strategic leadership into a formidable military instrument. Theater-level conventional or WMD warfare and unconventional warfare are not inherently incompatible. And unconventional or WMD forms of warfare will clearly be employed against one of our centers of gravity, the cohesion of our domestic and foreign coalitions. These forms of war also avert, minimize, or bypass a head-on collision with our high-tech precision weapons, aiming to create a favorable asymmetry for states who are willing to use unconventional or WMD forms of warfare.

Yet despite continuing debate over what threats we may actually face, it is not clear that we fully appreciate the realities of asymmetric warfare. One of the abiding myths of official U.S. strategic thinking is that our enemies will resemble us and fight our kind of war. Our enemy will be Saddam Hussein in 1990 for as long as we can see. Enemies will try to fight a high-tech conventional war using large conventional forces, precision-guided munitions, and electronic and information warfare, thus contesting us in areas where we are strongest. Thus it is more likely than not, in the official view, that our opponents will be states who are "peer competitors" of the United States rather than stateless guerrillas or terrorists. This view prevails as policy, though it is strongly challenged by many analysts.[26]

This policy exists even though the whole world learned from DESERT STORM not to fight us *exclusively* on our terms. For instance, U.S. Navy Captain James FitzSimonds of the Office of Net Assessment of the Office of the Secretary of Defense suggested that the asymmetric threat of an opponent waging a war of attrition against us is unlikely since no opponent would deliberately and voluntarily demodernize his country to fight a war entailing high casualties on both sides. Likewise, according to Captain FitzSimonds, "demodernization is not commensurate with

the prospective image that a great power would want to put forth."[27] This observation ignores the wars of Vietnam and Algeria, and a host of other colonial wars in this century, not to mention the World War II partisan wars cited above. It also ignores the strategic imperatives that take over when state and national survival are at risk. But this strategic myopia and insularity are all too characteristic of our military thinking and policy.

Likewise, while a more conceivable form of asymmetric response is the resort to nuclear or other WMD strategies, Captain FitzSimonds disparages this response as being born of military impotence and despair and again as being incommensurate with the image a great power wants to project. Here again the fact that an enemy might decide its survival is at stake and act accordingly seems to elude FitzSimonds. Finally, the real, and apparently only, danger he discerns is an enemy taking available technology and using it in a conventional high-tech manner to exploit our vulnerabilities. In other words, high-tech cruise and ballistic missiles, ASAT platforms and weapons, and weapons against our telecommunications and remote sensing devices are the main danger and threat to us.[28]

When we view each of these possibilities of asymmetric threats, it becomes clear that FitzSimonds' vision (and one assumes he speaks for his superiors) of future war is troublingly ethnocentric and complacent. For example, let us consider protracted war. It has long been known that low-intensity conflict, guerrilla war, etc. exemplify a protracted war strategy that consciously involves the risk of high casualties for both sides over a long time. It is chosen by technologically inferior forces precisely to minimize that weakness' impact and attack not where the enemy is strong but where he is weak. More importantly, in our time, many such attacks against modernized industrial or post-industrial states succeed.

Israeli Brigadier General (res.) Aharon Levran, a senior intelligence officer, recently told an interviewer that,

> You don't need heavy weapons to win. When you consider what has happened to us, the Palestinians have succeeded in beating us with the lightest of weapons. Clausewitz defines war as gaining one's goals. And when you consider what the Palestinians have done—the territory which they have gained—they truly have demonstrated that terror is not only simply a nuisance—**it is in and of itself a strategic threat**. We have already seen how short range light weapons, when used to carry out a campaign of terror, can be just as effective in achieving the Arabs' goals as heavy weapons. After all, terror has achieved something which, traditionally, one side only loses after a crushing defeat—territory.[29] (emphasis added)

An analogous outcome seems to be developing in Lebanon, where Israel seeks to end its 20-year military intervention there due to the incessant pressure of Hezbollah guerrilla warfare using mortars and low-tech weapons. According to Ehud Ya'ari, a respected Israeli military-political analyst, this turn in Israeli policy will be taken abroad as a sign that one can win by using simple weapons and keeping one's distance from the Israeli Defense Forces. Furthermore this denouement can also suggest that escalation is no longer a feasible response to this kind of warfare. Strong conventional military forces like those of Israel and the United States can no longer resort to escalation when facing such contemporary manifestations of low-intensity conflict.[30] The IRA's success in forcing its way into negotiations for Northern Ireland and winning substantial compromises points to a similar outcome, mocking the complacent assertions that we have little to worry about from such threats.

We should consider as well the warnings of K. Subrahmanyam, the former Director of India's Institute of Defence Studies and Analysis and one of India's leading strategists. He notes that India has been subjected to covert external aggression since 1983 that has eroded the distinction between external and internal security threats and made covert internal war a legitimate foreign policy instrument of certain nations. Moreover, such war is now

becoming a norm in many parts of the world, not just India.[31] Foreign interventions now use not just men, money, and weapons obtained from abroad, they also use narcotics or professional mercenaries as weapons of war. Foreign regimes can and do deliberately incite restive ethnic minorities on the other side of the border to paralyze the enemy's domestic security. Similarly, organized crime can become an instrument of transnational subversion. Such covert war is a cost-effective option for subverting, fragmenting, and destabilizing an enemy country and allows those launching the war to maintain strong conventional defenses against that enemy to prevent it (which may be a stronger conventional power) from retaliating and winning a quick, decisive victory. High-tech and low-tech capabilities go together as part of an overall strategy of protracted war where IW and the RMA can play useful roles.[32]

Alternatively, a state may not be strong enough to prevent transnational ethnic or criminal movements from using its land as a base for the incitement of conflicts elsewhere. Thus these elements penetrate it, use its conventional forces as a shield, and obtain a kind of sanctuary for their activities.[33] It should be noted that Subrahmanyam does not here mention IW and its uses in this kind of war which are many and telling.

These illustrations reveal once again the misguided nature of any strategy of modern war delinking war and politics and assuming conventional warfare is a thing unto itself. Clearly conventional warfare can fit well with low-intensity asymmetric threats as an actual reality as in the examples cited above, or in Chechnya and Afghanistan. Or it can be successful in its own right as in French Algeria, Israel, and Northern Ireland. Moreover, in all these cases either high-tech or media warfare played no small role in the conduct of the war and the achievement of victory.

Unfortunately, this misreading of the nature of the threat we and others already face conforms to the strategic

requirements of the U.S. position. As the 1997 National Military Strategy states,

> As a global power with worldwide interests, it is imperative that the United States be able to deter and defeat nearly simultaneous, large-scale, cross-border aggression in two distant theaters in overlapping time frames, preferably in concert with regional allies. . . . In this regard, a particularly challenging requirement associated with fighting and winning major theater wars is being able to rapidly defeat initial enemy advances short of their objectives in two theaters in close succession, one followed almost immediately by another. Maintaining this capability is absolutely critical to our ability to seize the initiative in both theaters and minimize the the amount of territory we and our allies must regain from aggressors. Failure to halt an enemy invasion rapidly would make the subsequent campaign to evict enemy forces from captured territory much more difficult, lengthy, and costly. Such failure would also weaken coalition support, undermine U.S. credibility, and increase the risk of conflict elsewhere.[34]

This excerpt perfectly exemplifies the efforts of U.S. strategists to formulate an operational template that converts technological superiority into operational concepts for gaining rapid decisive strategic superiority and victory. These concepts are also the foundation of the armed forces' *Joint Vision 2010* that aims to provide an operational template of future wars.[35] Several other key concepts of critical importance for understanding the strategic implications of new forms of war emerge from an analysis of this U.S. template of future war

The excerpt shows that the imperative of converting our technological and informational superiority into enduring strategic victory is tied to three key points in our strategy. These points are (1) our refusal to prepare for anything other than short wars, (2) the belief that we cannot achieve public support for prolonged conflict and thus must win quickly or else, and (3) the fragility of allied coalitions. Our strategy seeks to convert technology into force as quickly as possible and therefore is predicated on the possession of

strategic agility and forward presence. Those concepts mean that we can move everything quickly to a welcoming forward base or bases from where we can launch our preferred kind of war and halt the enemy's advance before taking the initiative for ourselves.

In fact this is a call to refight DESERT STORM against a future opponent who may not be so negligent about denying us our foreign presence or about striking at the heart of our coalition and strategic agility. The notion that our agility will be so overwhelming as to negate the threat to our foreign presence overlooks not only the current shortfalls in manpower, readiness, and lift afflicting the armed forces, it also neglects the true history of the Gulf campaign.[36] Whatever else airpower can do, it cannot defend itself or its bases. Nor do command of the air and air superiority guarantee victory in low-intensity conflicts, as Chechnya shows. In 1990 Iraq failed to move deeper into Saudi Arabia to deny us both forward presence and strategic agility.[37] With future enemies taking note, it is unlikely that we will again have opportunities to undertake a deliberate buildup of the theater or sufficient access to bases for the use of our long-distance platforms.

Thus in future wars true jointness will be necessary, entailing a large, not quick, buildup of forces. It likely means a longer war than we want and one in which seizing territory is of immense importance because we have the political responsibility of defending the territory of our coalition partners and allies as well as our forward presence and platforms. Those requirements logically entail serious consideration of the Army as an occupying, constabulary force and of the decisive shaping of the occupied territory's political future. This is precisely the kind of question that military commanders do not want to confront and which make political leaders hesitate before acting decisively. We seek to avoid the choice by wishing it out of existence in our strategy.

In our template of future war, we assume that we will know when an attack occurs, who launched it, and the true target. We will have informational certainty that overrides the potential for "fog." We will also have technological superiority to be able to achieve this certainty. Moreover, we will be able to move quickly to "the scene of the crime" and proceed to fight back. However, as previous war games demonstrate, our leaders are often unable to determine who is attacking us and how.[38] Worse yet, the spread of IW capabilities adds to the difficulty of tracking down aggressors in cyberspace. It will not only be more difficult to know for sure what has happened to us or who gave the order and who actually did it, but it is not even clear if such actions directed against our own infrastructure constitute acts of war that can justify military responses.[39] If speed is of the essence in future war, the absence of tactical warning and the uncertainty in deciphering the elements of attack strike directly at our ability to respond decisively in timely fashion at the strategic level.[40] For example, is it merely happenstance that as the crisis with Iraq reached its apogee in February 1998 the Pentagon reported an unprecedented number of untraceable attempts to invade its computers? Neither is it likely that our coalition partners will be enthralled with our inability to attain a decisive determination of whether or not they were attacked

Nor is it foreordained that we will have control over what our own and foreign news media will see, hear, and know. Developments in telecommunications allow reporters and media to be on the scene almost instantaneously, preempting the intial government construction of events. The international news media are now a globally available system of information dissemination that is more or less equally accessible to all sides in any conflict, largely independent of government. Indeed, our own media have a built-in suspicion of government efforts to muzzle or deceive them or to spin what we see. Thus we cannot take for granted, as we now do, that we will have uninterrupted control of what goes over the media. Certainly the fiasco of

the U.S. government teach-in at Ohio State University concerning the February 1998 Iraqi crisis shows the double-edged nature of the media's sword.[41]

Finally, it is not clear that we fully understand the strategic political consequences of what we are creating. Clearly the RMA places would-be peer or niche competitors like Russia under enormous pressure against which they already are rebelling. They may understand the strategic implications of our actions better than we do precisely because of their vulnerability and backwardness *vis-à-vis* the United States. Precisely because they are among those who feel most threatened, they see the threat in radically different ways than we do. And if it is true that victory goes not to the big battalions or to the technically superior force, but to the force that can control the definition of the battlefield, it is entirely possible that we could even defeat Russia decisively in battle yet fail utterly to achieve whatever strategic goal we have chosen.[42]

Perhaps because they see the threat in all its dimensions more cogently or at least differently than we do, they can respond by redefining the battle away from ways that accrue to our superiorities, e.g., by going nuclear. However, that is only one among many options. Russia's threat of going nuclear can alone dissuade many opponents from exploiting its current weakness.[43]

Our own operational doctrine and strategy emphasize attacking first, even preemptively, with conventional and informational weapons. They also stress that the cohesion of the enemy government and hence of its society is the center of gravity that we aim to degrade. No self-respecting enemy will wait for us to strike first and possibly end the war along with his ability to function. He will seek to challenge us, probably preemptively. He could resort to WMD weapons, low-intensity conflict, or other asymmetric threats that we do not handle well. As a recent game indicated we are badly prepared for a nuclear attack. Players found that despite years of training, they were

unprepared for the pandemonium, the interagency sniping, the conflicting intelligence reports, and the constant leaks of half-truths. it is not surprising that here, as in a Rand Corporation game, the result was "a sense of bafflement and frustration."[44]

This consideration raises a more general point. Everything we see about U.S. operational doctrine breeds a high degree of aggressiveness up to and including preemption. Yet at the same time the nature of IW frequently makes it very difficult to know whom to attack or counterattack, leaving us with that bafflement and frustration. Therefore IW used on us, e.g., blinding our satellites or computer systems, deprives us of key operational capabilities that we have always assumed will be available to us. IW or asymmetric forms of war that are preemptively used against us because we threatened to use them against the enemy preemptively will surely throw our operational and strategic doctrines into disarray, constituting strategic surprise against us. Thus our resort to preemption or to the publicly voiced thought of acting preemptively almost certainly will lead not just to retaliation in kind but also to an effort to wrest control of the escalation ladder away from us. That effort to take escalation control away from us will be even more likely where a state lacks our formidable conventional military power. Hence, as in Russia's case, we find the overt threat, stated in Russian doctrine, to go first with nuclear weapons should attacks occur against key installations. Even if the attacks are purely conventional, the first-strike or even preemptive nuclear option has already been invoked in Russian doctrine.[45] Our enemies' fear of being preempted in a war where the first strike can be the only strike should inevitably lead them to race to preempt us. As Stephen Cimbala writes,

> the revolution in military affairs could help to undo itself if it creates sufficient fears on the part of . . . nuclear nations that their capabilities will be subject to timely and decisive preemption *whether or not they have have threatened explicitly*

> to use nuclear weapons against regional opponents. . . . However, counter-proliferation runs the risk of creating anticipatory US allies and dependencies beyond the reach of timely American reinforcement.[46]

Therefore the quest to attain technological superiority and transform it into lasting operational and strategic superiority and decisive outcomes easily translates into a race to achieve strategic surprise to negate the enemy's technological superiority. Pearl Harbor is a perfect example. Japan had no realistic chance of defeating the United States and knew it, in large part due to our technological and economic superiority. Yet Tokyo thought that by achieving what it hoped would be a dissuasive strategic surprise it could force us to take Japan seriously and come to terms with it. Worse yet, we had more information about the upcoming attack than virtually any attacked nation has had before or since, and we failed to do anything with that information. Fog, friction, etc. clouded our understanding and resolution.[47]

Since there is no reason to suspect that the speed of strategic-level command decisionmaking relative to an operation has increased in our government since 1941 (and perhaps when including our allies it has decreased), we will probably once again be surprised as in Somalia and Lebanon and in our initial efforts against Haiti; and as Kuwait in 1990, Israel in 1973, and Russia in Groznyi in 1994-96 were repeatedly surprised. Indeed, surprise is a chosen weapon of the technologically inferior. Our effort to transform technological superiority into lasting advantage will surely generate a counter-race to preempt and surprise us. Given Russian studies of IW and the RMA, we should not be surprised if the first act of a war would be one of which we were entirely unaware.

Indeed, there are a number of reasons why our vaunted informational and intelligence capabilities may not be as brilliant as advertised. First of all, many senior U.S. officers and policymakers have voiced loud and repeated complaints

about the overly secret and bureaucratized intelligence process which provides intelligence that is often either useless or late.[48] Robert Steele argues that,

> The U.S. intelligence community does not have the long-term ethnic human penetrations it needs against international criminal or terrorist organizations, nor does it possess the kind of tactical SIGINT capabilities, or even air-breathing tactical IMINT, that would be helpful in coping with these challenging international threats. Cultural movements baffle "Western'" technical indications & warning (I&W) systems because they do not use point to point communications but rely instead on couriers, the pulpit, and broadcast television indirectly to mobilize action elements from the masses. The U.S. does not have an electronic counter-intelligence capability worthy of the name, nor has it established the most basic economic counter-intelligence capabilities. [49]

Nor is our record of understanding Russian goals, intentions, and capabilities any better. Indeed, one recent study on surprise in warfare notes that even when states who suffered surprise attacks changed their view of the enemy's intentions before the attack, they proved unable to adjust their view of enemy capabilities and were always victimized by their belief in their own superiority and the effective inferiority of the enemy.[50] Given the visible hubris that disfigures contemporary American military writing and thinking, the likelihood of our being surprised by enemy capabilities, if not ultimately by his intentions, is a very real one.

What makes this race for preemption and surprise particularly worrisome is that we have only one bite at the apple. Historically those states that relied on technological superiority or on strategic surprise to provide them with a decisive and lasting victory had to operate under severe time constraints. This was true for Germany in both World Wars, for Israel in 1967, and for the Arabs in 1973. In most of these cases, surprise failed to achieve the knockout blow. Instead, a force optimized for fast-paced, intensive, but brief war was drawn into a protracted one which it could not win

or which exacted enormous costs and domestic dissatisfaction. Since our strategy openly and consciously strives to avoid protracted war, it paradoxically appears to risk that outcome by its emphasis on avoiding that outcome more than would otherwise be the case. If we optimize a force for one strike and out, admitting that otherwise we will not demand sacrifices, we probably will end up demanding much more from ourselves and our allies for little gain.

What aggravates the strategic dilemma of surprise is our failure to ponder the distinction between limited and total or unlimited war. By making the war a total one for our enemies and approaching them from a posture of conventional and nuclear superiority and an announced intention to preempt, we give them almost no choice but to wrest the element of surprise from our hands. If both sides are racing for technological or strategic surprise, the outcome is as likely as not to be a stalemate, i.e., protracted war of attrition, the exact opposite of what we want and our greatest fear. If we fail to realize what our stated military objectives logically entail and do not alter them or our thinking, we will probably fail in our strategic quest.

In a future IW or RMA war, we will not have the luxury of being a privileged sanctuary, where we can be the arsenal of democracy for others while they fight. Let us remember this kind of war erases distinctions between front and rear. The entire state is now a legitimate target. Since today we define national security in all-encompassing ways to include not just defense, but social, ecological and economic security, anything can be attacked in the guise of degrading that security. Our homeland is now a potential target, and homeland defense is no longer an option we can renounce.[51] As a RAND war game and ensuing study showed, our enemies will relish opportunities to attack us here and abroad below the threshold of triggering massive retaliatory U.S. actions and will often successfully elude detection and response. Our great vulnerability to such attacks led players in the RAND game to exercise extreme caution concerning escalation options, the heart of our

strategy. This caution also reflected unforeseen friction, the result of strategic surprise, and a lack of tactical warning.[52]

Because the United States, like its potential enemies, is no longer a sanctuary, political dissidents, our media, criminals, terrorists, etc. become even more legitimate instruments of war, while our civilian structures become even more tempting targets. Our vulnerability to surprise attacks whose origin remains murky deprives us of the capability to launch our kind of war and shows our strategic vulnerability to both surprise and homeland attacks.

One should not think that in a future war we can tear apart the enemy but escape retribution because of our speed. We rely on one quick overwhelming blow and the unverified belief that our superiority will be so demonstrably crushing as to obliterate any reason for resistance. Such thinking is extraordinarily optimistic about mechanizing, automating, and rationalizing war to our tastes. Although our strategists are well aware that adversaries may try asymmetric war using weapons of mass destruction or low-intensity or unconventional methods, they disparage those possibilities; there seems to be little awareness of the significance of the issues of preemption and of total war that arise out of our strategy. Precisely because for our enemies the war may be total and not limited, they will race to preempt us.

Therefore another option for them is to remove our capacity for preemption by announcing in advance the will, if not the actual capacity, to put their WMD on automatic pilot or fail-safe capability, so that if their C4I is disabled, the dead hand will inflict unacceptable damage upon us or our allies.[53] Russia already has such a nuclear capability, and it is relying ever more on nuclear missiles, both strategic and tactical, for even tactical contingencies.[54] Of course, we could then retaliate in kind but by doing so we would only assume responsibility for the post-nuclear aftermath while we made the rubble bounce.

It is easy to underestimate this danger. Russia's tactical and strategic nuclear weapons are associated with a high degree of pre-delegated launch authority and local control. The strategic systems are known to be on a launch on warning (LOW) concept. Were the control systems for either the strategic or tactical systems disrupted, commanders might operate independently and launch nuclear strikes. Moreover, Russia's present doctrine lowers the nuclear threshold quite deliberately, given its absence of usable conventional power.[55] Thus preemptive or accidental nuclear or other WMD strikes (Russia apparently still has a large biological and chemical weapons program and cannot muster the money to dismantle the latter as it has agreed to do) are hardly unlikely contingencies in war, especially a total war.[56] Indeed, Russian doctrine is increasingly exploring the use of tactical nuclear systems as warfighting weapons as well as the use of strategic weapons for tactical purposes.[57] If one were to combine the dangers of surprise or preemptive attack with the possibility of nuclear preemption or retaliation, the war would quickly spin out of control. Since the whole thrust of our thinking about future war is to put it under our control, nuclear or other WMD scenarios strike at the very notion of such war. Such warfare would be not only unprecedented in its destructive scope, but also utterly unpredictable and perhaps uncontrollable. The reason why Russian planners invoke nuclear use against attacks by precision-guided and electronic weapons is that they view such attacks so seriously.[58]

In 1992-93 Russia replied to Turkish talk of going to Azerbaijan's aid in Nagorno-Karabakh by threatening nuclear war. The leader of Russia's Security Council, General Evgeny Shaposhnikov, stated that a Turkish invasion meant "World War III." The reason for this dissuasive threat, which did deter Turkey, was that war games had told Moscow that its conventional forces on the Armeno-Turkish border would lose to Turkey, thus opening Armenia to Turkish invasion. Absent usable conventional power, nuclear weapons became the sole instrument

available for use to dissuade or deter Ankara. This episode is instructive, for it confirmed that nuclear weapons are the weapons of the weak, and that post-nuclear capability in high-tech, EW, IW, and space capabilities are trump.[59] But it also confirmed that nuclear threats do deter and induce caution. It is likely that a similar threat against us would have an equally inhibiting impact upon our leaders, narrowing escalation choices as in the Rand game. But nuclear and preemptive options in the ether and cyberspace hardly exhaust the possibilities for asymmetric responses to American strategy.

Another alternative open to such asymmetric warfighters derives from what happened to Iraq after 1991. We do not take full account in our strategy of the fragility of enemy regimes—that if we beat them, the state implodes. Such implosions would present us with unforeseen problems whose magnitude far outstrips our capability to convert military victory into a stable and lasting political solution. This is as true for Iraq in 1991 as it would be for Russia or China if they lost a major war today. This state implosion, as in Russia in 1917-18, would leave us no choice but to occupy territories with millions of armed men. Victory could not be achieved without occupying much territory for without it the problem we had fought against would remain. The logical outcome of such an American "victory" would be a strategic defeat because we would be drawn into an interminable occupation role of an immense swath of territory with governmental responsibility for that land.

If our strategic target is the nerves of government and of the armed forces, we risk disassembling the entire state and society and then having the obligation to police it afterward, a clearly unviable strategic option. Yet we simply cannot walk away saying we had a job to do and we did it, so long. Indeed, in every war and intervention that we have conducted since 1941 we have had to sustain an enormous nation-building effort or else a large forward deployment of long duration in order to achieve our minimum strategic

objectives. There is no a priori reason to suspect that the future would be materially different in this regard.

It is worth pondering recent U.S. military operations where we had to conduct major constabulary operations alongside of or in place of large-scale combat operations. One quickly discerns that we are in big trouble, particularly if we have undone the basis of order throughout the invaded societies. In all these cases, Panama in 1989-90, Kuwait in 1991, Somalia in 1993, Haiti in 1994, and Bosnia since 1995, we find a failure to achieve our political objectives. And our checkered history in conducting such operations goes back at least to the planning for the postwar German occupation after World War II, which is acknowledged to be a debacle in planning from which the Cold War rescued us. As a recent surveyor of the post-1989 operations observes, "There may well be an important lack of connectivity between national policy, national strategy, theater strategy, and operations."[60] These failures were hardly unforeseeable. Destroying a political community brings about a return to anarchy which must then be overcome, often by force majeure. The disappointing aftermath of Panama, a technical democracy behind which high corruption continues, should be a cautionary tale to any U.S. leader who wants to take out a government.[61]

Similarly, in Kuwait there was a disjunction between the military strategy and the political strategy. The latter saw regional stability in an Iraq that remained intact but could no longer threaten its neighbors. Yet it was not foreseen that Iraq's Kurdish, Shiite, and Sunni Arab factions would all go to war with each other and drag us in.[62] Under the circumstances it is not surprising that Iraq rightly viewed our presence as an effort to dismember it and to do away with its ruler. And to couple this policy with an inspection regime that depended, like the Versailles Treaty, on the cooperation of the embattled and unbowed Iraqi government for compliance while we neglected to sustain our coalition can only be described as naive.

With regard to the February 1998 fiasco with Iraq, Jim Hoagland wrote that,

> [The] problem is the gap between the American military's vast destructive capacity and the limited ability of American political leaders to use it to shape definitive outcomes especially against Third World outlaw regimes. The American Goliath is loath to fight to complete victory in such a mismatch. Complete victory over a much weaker foe brings encumbering consequences for a moral nation. America's unwillingness to accept the responsibilities of victory lies at the heart of the paradox of a brilliant military campaign that seven years later is politically unfinished.[63]

Hoagland's insight returns us to the conundrum shaped by the asymmetry between our aim to fight wars that are fast and limited for us and the resulting total wars for our enemies. For them defeat means the end of the government and foreign occupation or dismemberment. Consequently if we beat Russia or its proxies while retaining our strategic focus, our forces will almost certainly end up trying to police a protracted civil or ethnic war, or an insurgency, or both. In this regard, the international experience of 1918-22 in the Soviet Union bears recalling.

Our post-victory wars for state stabilization will be inherently protracted, and once we are in them, we risk forfeiting foreign and domestic support and the use of strategic surprise based on technology to achieve a "liberal" outcome. Here we face the asymmetric threat of unconventional war that turns into attrition and protracted conflict where we are clearly vulnerable at the strategic level.

Russia's Strategic Environment and Perceptions.

While unquestionably any country would prefer to have our forces and problems than Russia's, the fact remains that the kind of complacency we display is often the harbinger of defeat, while insecurity, if nothing else, can sharpen the mind. Russian elites agree that their society faces multiple

threats. While policymakers cannot, in fact, decide upon priorities and formulate a coherent defense policy, there is little doubt that they face multiple, and some would even say, growing threats on a host of azimuths.[64] Given this context, informational threats that employ superior foreign technology hold out some potentially dreadful potentialities even in peacetime. In wartime these dreadful potentials are much greater because Russian observers understand the immense capabilities that reside in information technology and high-tech conventional weaponry. Although there is a substantial debate and many unresolved issues in Russian thinking about information warfare and future war, some things are quite clear already.

Russian writers have a much broader notion of information warfare than do American writers. They include warfare targeted against the minds and physiques of enemy combatants and even of whole societies. They see this form of warfare as ushering in a new series of weapon technologies that can strike enemies in wholly new ways, including biological or psychotropic weapons.[65] Many commentators, civilians, and military officials, e.g., former Chief of Staff Colonel General Viktor Samsonov, contend that IW proceeds during peacetime. Some writers demand a new definition of war to include this kind of bloodless, peacetime campaign against key political and informational strategic targets. Allegedly Russia has, for several years, been in an information war with the United States and the West. Moreover, in this view, Russia is losing or has lost that war. Its domestic anomie and loss of values reflect the West's successful targeting of the Russian media, who, as servants of the West, have betrayed Russia.[66] Furthermore, Russian writers also believe that IW carried out against their conventional or strategic fores can undo strategic parity and stability. Therefore an IW attack practically forces Russia into a retaliatory nuclear first strike that negates our basic strategic premises.[67]

Many of these ideas and perceptions turn up in Russia's 1997 security blueprint stressing internal threats,

including threats to Russia's spirituality, morale, and moral integrity.[68] Other officials, like Foreign Minister Yevgeny Primakov, evoke threats to Russia's intellectual, communications, or information space.[69] The discussion about an intellectual or ideological threat is pervasive, even if assessments vary. While this discourse on an informational threat reflects Russia's profound disenchantment, it does not necessarily entail the sense of being presently in an information or psychological war.

But those disaffected elites who believe this war is occurring are updating Lenin's notion of constant political or ideological warfare with the West to our time and openly raising the Leninist-Stalinist notion of internal enemies. Internal political opposition equates to sabotage, opening the way to a domestic war. War at home and war abroad could become a seamless web. Information warfare provides scope for political and military conflict beyond anything we can envision, targeting whole sectors of societies through what used to be called "the hidden persuaders." Current U.S. claims on behalf of its IW capability betray a touching innocence about its strategic potentialities in troubled societies and about the nature of war in general.[70] Such posturing only fuels Russian paranoia. These new weapons could, in the Russian definition, include whole series of biological or psychotropic weapons, or simply novel uses of information and other technologies to destabilize a society from within.[71] Russia is still devising biological and chemical weapons which could play an enormous role in this context. We must increase our powers of empathy, realizing that for other cultures information warfare, as they understand it, is a radical, even revolutionary, development that puts their whole society at risk and makes it the center of gravity. The Russian perception of such a threat makes many more contingencies possible and converts the unthinkable into the conceivable.

Friction and Coalition Warfare.

There are other reasons why our vision of future war is not nearly as roseate as it seems. Barry Watts has demonstrated the extent to which friction survives in warfare notwithstanding the brilliance of our 1991 campaign in the Gulf.[72] We can assume, as in Somalia or even in the early-1998 Iraqi crisis, that the unforeseen over-exertion, fatigue, and communications breakdowns will continue to affect war at all levels. The claims made by proponents of advanced technology about the dispelling of fog and friction are fanciful and unproven. Though they are aware of the problem of information overload, the promise of warfare without human encounters obscures the fact that human beings will still control war and still be prone to all the dysfunctional behaviors and failings of past warriors under stress. Human nature is not a Lego piece that we can insert or remove at will from the military equation.

But the problems of friction go deeper than that.[73] As Watts points out, Clausewitz first uses the word friction to denote bureaucratic obstruction and intrigues. These are the daily stuff of bureaucratic politics even under the best of circumstances.[74] For example, we now see in the Pentagon a clash between those who who want to destroy enemy computers and those who want to listen to them, using the information gleaned thereby for intelligence purposes. Each side has compelling arguments. But even in 1991, conflict between the military who wanted to attack and the intelligence agencies who wanted to listen created friction between them which certainly affected the conduct of military operations.[75]

Moreover, the Pentagon is now devising weapons to attack enemy computers actively to reduce the amounts we must spend defending our own information systems from enemy attack. Evidently it takes more people to defend the numerous assets threatened by cyber-warriors than it takes to be such a warrior. Since any system with more than one computer is vulnerable, all systems are vulnerable. An

active offense is crucial to self-preservation and self-defense of our information systems. Furthermore, defense of information, or operational security (OPSEC), increases rather than decreases the number of people needed to perform the mission, and they must all be trained professionals. Does this mean we can confidently expect legions of volunteers to spring to OPSEC missions in place of soldiers who are needed elsewhere when we cannot even distinguish who is attacking us and why? Such considerations suggest that the human factor will become more important, certainly with regard to quality and perhaps to numbers.[76]

Since the threat to our computer systems is ubiquitous, and since the best defense is a good offense, we are building up for an active global offense. We must resort to preemptive electronic assault on those identified as planning or who are prepared to penetrate key computer networks. That assault would, as in the initial phase of 1991, combine EW with air strikes using specially treated munitions. But, as was shown earlier, we cannot achieve the requisite level of tactical, let alone strategic, warning. Nor can we overlook the consequences of what our efforts to preempt will lead our enemies to do. Thus bureaucratic friction impeded operations in 1991 and has now led us into uncharted strategic waters.

We now confront several alternatives. The necessity for choice will inevitably increase bureaucratic friction, if not fog. We can simply absorb the first blow and do violence to our own strategy of going first in force. Or we can create weapons and forces to target either unidentifiable hackers or cyber-warriors as in the wargames that Fialka and the Rand Corporation cited.[77] Or we can launch preemptive strikes to destroy an enemy's computers and C4I, leading us back to the unacceptable strategic outcomes discussed above.

Other examples of friction clearly arose in other games using IW. The Rand Corporation game found that not only

did we lack adequate tactical warning of cyber attacks or identification of who the enemy was, the bureaucrats in the game could not agree on whether suspected cyber attacks constituted an act of war or discover whether these attacks were at the limit of an enemy's capability. Many players were frustrated by the lack of adequate strategic intelligence—a prime example of friction and fog—directly refutating the confident forecasts of many writers on RMA who assume near perfect knowledge. Such uncertainty "crippled the administration's capacity to take decisive action."[78] It is thus quixotic to believe that the empty or cyber-dominated battlefield will lack friction and fog, or that it will find unanimity among commanders in the field or back at headquarters, as to what is going on.

Still other occasions for friction exist. It is an axiom of contemporary politics and military thinking that in future contingencies we will normally take part only via military coalitions. While we have a rich history of participating in such operations, we have insisted, not always wisely, that we alone must lead them.

Anyone who has ever participated in a simulation, game, or exercise involving a coalition, or who has understood the troubles we had and have in Bosnia, Kosovo, and Iraq, will understand that coalition formation is not part of our strategic genius. Our insistence on unilateral leadership and our ethnocentric disdain for foreign insights, interests, capabilities, experience, and skills already suffice to make coalition formation a process replete with friction and fog. Meanwhile our allies are under no a priori obligation to heed our wishes or share our objectives. In the current Iraqi and Kosovo crises, many of our allies strongly disagree with us. Likewise, in 1991, it was concern for the cohesion of the coalition made up of other Arab states that led us to abjure a march on Baghdad. Clearly coalitions which must be coordinated among many governments, each of which is now a ramified series of bureaucratic networks that are themselves prone to all the pathologies of bureaucratic

politics, will inherently create the friction, discord, delay, misinformation, fog, etc., that Clausewitz knew all too well.

For example, the entire question of foreign presence is subject to the wishes of the coalition's partners, as stated in treaties, laws, and our executive agreements with them. If they deny us that presence, our entire strategy is then severely weakened. Or if they are attacked first, as in 1990, and our enemy can deny our entry into the theater, other states might well think twice about joining us. Obviously these contingencies will force us into a prolonged conflict, reduce our agility, force us to alter our strategy in fundamental ways, and have secondary and tertiary repercussions that we cannot fully predict. For example, we might have to call in more troops and mobilize the reserves, thereby precipitating an even more intense domestic debate.

The coalition aspect of future war also provided some of the most aggravating experiences of the Rand Study, which suggests that we have serious future problems here. First, apart from the normal bureaucratic and political friction in all states, many of our allies are equally vulnerable to untraceable attacks on their information systems and probably lack some of our intelligence resources. So they too will have comparable problems maintaining tactical and strategic intelligence capability, warning, and strike capability. Many allies might also have serious infrastructural or political vulnerabilities that will not only impede their decision-making, but may also deflect them from joining us or take them out of the picture altogether. If there are severe political issues in these states, which may be undemocratic, we may end up wasting valuable time and effort in trying to broker political deals within them before getting agreement on key coalition issues. Such diversions will weaken strategic unanimity concerning operations and strategic goals.[79]

The fundamental error of the so-called "Millenarian school," those who see the RMA literally as the functional

equivalent of a magic bullet, is that they assume first that all relevant decisionmaking in war is either operational or tactical at the battlefield level and have factored out strategic political considerations.[80] For them, politics no longer exists in the world of the RMA, or, if it does, communication is equivalent to decision. Despite the fact that the RMA has undoubtedly accelerated the speed at which information travels and the amount of information available to commanders, it has not appreciably quickened strategic and political decisionmaking. All commanders have access to much of that information, and the more information key players have the more power and opportunity they all have to check each others' decisions and impede strategic decisionmaking. The political process, especially in a large democracy, is intended to be slow-moving and can be expected to remain so.

Thus the Millenarian vision fails to account for the impact of coalitional warfare in particular or politics in general on the conduct of military operations. In the worst tradition of previous failed U.S. endeavors, the Millenarian concept of war divorces operations from strategy and fails to focus on anything other than the operational missions involved in destroying the enemy's forces and information networks. This separation of strategy from operations, of the political objectives from the military means, pervades both our civilian and military elites, who seem unable to talk to each other openly. Hence there is mutual suspicion and disdain on both sides of the fence as well as a strategic culture of mutual mistrust among them.[81] Thus the Millenarian vision falls prey to the vice of strategic ethnocentrism and to a dangerous insouciance concerning war against opponents who have their own ideas about how to fight modern war.

Conclusions.

The operational concepts to which we are gravitating do not provide us with sufficient clarity concerning strategic

goals. We could win brilliant military victories only to fall prey to strategic obligations that were not even foreseen before the war began. Worse yet, as games suggest, we may not be able to bring our force to bear as planned and end up in a protracted war or conflict of attrition both in cyberspace and battlespace.

The great failing of most U.S. security thinking, and even about the RMA and IW, is that it remains confined to the operational level of war, focussing on the indispensable but insufficient task of defeating the enemy decisively. If the objective of war is a better peace and the realization of political goals, than our current thinking about war does not face that issue. We also evade consideration of what the enemy might do. Our capability for achieving decisive military success is taken for granted. Yet this axiom, that we can deliver rapid decisive strikes to obtain our objectives, is paradoxically at odds with our political processes. As we have seen above, victory often brings responsibilities that are unwanted, burdensome, and antithetical to our strategy. In other words, our operational doctrine misreads strategic realities.

Increasingly, the Army, the other services, Congress, and often the media demand that the administration announce an exit strategy, a desired end-state, and a guarantee of rapid victory before committing to arms. Our strategy aims as much at our own news media as at the media of other states. In fact, our strategy is disingeneous because such guarantees in advance are plainly unthinkable.[82] Our strategy in fact amounts to a call for a zero-defects security and defense policy. Yet simultaneously we proclaim that we are building a generic military that will achieve superiority across the spectrum of conflict even when we have no idea of our goals in any of those future conflicts.

The focus on technological superiority cannot ensure international security. True, it may secure the armed forces against domestic challenges from the media, the public, or

other branches of government by claiming the ability to guarantee a victory in a short war with no casualties provided the civilians let us manage it. But paradoxically, it restrains our ability to meet future challenges credibly.

Finally, this uniquely American strategy ignores the strategic context facing other states and assumes the capability of victory for our forces throughout the entire spectrum of conflict. Even as it is a totalizing and universal theory, aiming to give weight to our Wilsonian and moralistic urge to punish bad governments around the world, the new vision of war remains ethnocentric and divorced from true global reality. In a television interview concerning the Iraq crisis of February 1998, Secretary of State Madeleine Albright stated that "if we have to use force, it is because we are America. We are the indispensable nation. We stand tall. We see further into the future."[83] Nor are Albright's views confined to the State Department alone. Rather, in their suggestion that we need not heed foreign concerns, they reflect deeply held views within the military.[84] Unfortunately for those who hold such views, we are not talking about a John Wayne movie but about the inherently unpredictable realm of war where hubris generally pays a heavy price. Along with such hubris goes a corresponding misunderstanding of war and force. Secretary Albright said to a college audience in Tennessee, "We are talking about using military force, but we are not talking about a war. That is an important distinction."[85] It certainly is not a distinction to Iraq. Once a nation starts using force, it cannot tell where it will end, for where does force end and war begin? Unfortunately, the conjoining of the quest for technological superiority and one first strike do not augur well for success in present or future crises. A recent study of the strategic goals of our foreign policy revealed that there were "enormous areas . . . of deficiency in the conduct of international affairs in terms of clarity of goal, clarity of purpose, and any close alignment of those goals to those purposes."[86]

Such troubling strategic thinking is rooted in a uniquely American tradition that separates war from peace and operations from strategy, disdains the lessons of history, and believes in technology and massed firepower as a ready answer to all wars. It assumes our enemies inferior and on the brink of defeat before we set foot on the battlefield. It assumes that we are giants and that everyone else will fall or accept us. Yet while it may be wonderful to have a giant's strength, history shows that using it effectively is another matter altogether.

ENDNOTES

1. U.S. Army, *Operations, Field Manual* 100-5, Washington, DC: Headquarters, Department of the Army, 1993, p. iv.

2. "USA Conventionally Challenged by Saddam's Hidden Weapons," *Jane's Defence Weekly*, November 19, 1997, p. 19; "The Big Question: Can Saddam Be Beaten by Bombing Alone," *Jane's Defence Weekly*, February 25, 1998, p. 20.

3. Mary Fitzgerald, "Russia in 2025: Will It Be an RMA Power?" *Beyond the Technological Frontiers of Force XXI, Final Proceedings of an Army After Next Project Conference*, Atlanta: Georgia Institute of Technology, Center for International Strategy, Technology, and Policy, 1996, pp. 15-18.

4. Ralph Peters, "Spotting the Losers: Seven Signs of Non-competitive States," *Parameters*, XXVIII, No. 1, Spring, 1998, p. 36; George and Meredith Friedman, *The Future of War; Power, Technology and American World Dominance in the Twenty-First Century*, New York: St. Martin's Griffin, 1998. The title alone spells out the prevailing mood.

5. Admiral William T. Owens and Joseph Nye, "America's Information edge," *Foreign Affairs*, LXXIV, No. 2, March-April, 1996, pp. 20-36; Admiral William A. Owens, "The American Revolution in Military Affairs," *Joint Forces Quarterly*, Winter, 1995-96, pp. 37-43.

6. Colonel Charles M. Westenhoff, USAF, "Airpower and Political Culture," *Airpower Journal*, XI, No. 4, Winter, 1997, pp. 44-47. This kind of service boosterism is by no means confined to the Air Force. Army writers generally claim that land power, which they can rarely

define, is the decisive arm of war, just as the Air Force makes the same claim for air power.

7. Colonel General N. A. Lomov, *The Revolution in Military Affairs: A Soviet View*, trans. and published under the auspices of the United States Air Force, Washington, DC: U.S. Government Printing Office, 1973; John Erickson, Edward L. Crowley and Nikolay Galay, eds., *The Military-Technical Revolution*, New York: Frederick A. Praeger Publishers, 1966; William R. Kintner and Harriet Fast Scott, trans. and eds., T*he Nuclear Revolution in Soviet Military Affairs*, Norman, OK: University of Oklahoma Press, 1968.

8. *Ibid*.

9. Peter Pry's unpublished manuscript, *War Scare*, gives telling evidence of Soviet intentions for a first-strike that would have been both conventional and nuclear in nature.

10. Stephen J. Blank, *The Soviet Military Views Operation DESERT STORM: A Preliminary Analysis*, Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War college, 1991, pp. 31-33.

11. George F. Kennan, *The Decline of Bismarck's European Order: Franco-Russian Relations, 1875-1890*, Princeton, NJ: Princeton University Press, 1979, pp. 350-366. President Eisenhower also understood this when facing calls for a preventive war against the Soviet Union.

12. Norman C. Davis, "An Information-Based Revolution in Military Affairs," in *Athena's Camp: Preparing for Conflict in the Information Age*, John Arquilla and David Ronfeldt, eds., Santa Monica, CA: Rand Corporation, 1997, pp. 84-86; "The Information Edge: America's Non-Nuclear Deterrent," An Interview with Former Secretary of Defense William Perry, *New Perspectives Quarterly*, June, 1997, p. 45.

13. Steven Metz, "Racing Toward the Future: the Revolution in Military Affairs," *Current History*, April, 1997, p. 185.

14. *National Military Strategy of the United States*, 1997 located at www.dtic.mil/jcs/nms/executiv.htm (henceforth NMS), Owens, pp. 37-43; General John M. Shalikashvili, *Joint Vision 2010*, Washington, DC: U.S. Government Printing Office, 1997; Joint Chiefs of Staff, *Concept for Future Joint Operations: Expanding Joint Vision 2010,* Washington, DC, 1997; *Report of the Quadrennial Defense Review* (henceforth QDR), Washington, DC, 1997, pp. 39-42; Benjamin S. Lambeth, "The Technology Revolution in Air Warfare," *Survival*, Vol.

XXXIX, No. 1, Spring, 1997, pp. 65-83; Colonel Richard Szafranski, USAF, "Parallel War: Promise, Problems," *Proceedings of the U.S. Naval Institute*, August, 1995, pp. 57-61; Harlan K. Ullman, James P. Wade, *et. al*., *Shock and Awe: Achieving Rapid Dominance,* Washington, DC: The Center for Advanced Concepts and Technology, National Defense University Press, 1996; Daniel Goure and Stephen A. Cambone, "The Coming of Age of Air and Space Power," *Air and Space Power in the New Millennium*, Daniel Goure and Christopher M. Szara, eds., General Ronald R. Fogelman, USAF, Foreword, Washington, DC: Center for Strategic and International Studies, 1997, pp. 1-47; Alvin H. Bernstein and Martin Libicki, "High-Tech: The Future of War?" *Commentary,* January, 1998, pp. 28-31.

15. This refers to the essays of John Warden, which have reportedly been "canonized" by the Air Force. For a full listing of these sources, see Szafranski, p. 61; Colonel John A. Warden III, *The Air Campaign: Planning for Combat*, Washington, DC: National Defense University Press, 1988. For a critique of this view, see Mark M. Clodfelter and John M. Fawcett Jr., "The RMA and Air Force Roles, Missions, and Doctrine," *Parameters*, Vol. XXV, No. 2, Summer, 1995, pp. 22-29, and the sources cited there.

16. See note 14.

17. *Ibid.*

18. TRADOC Pamphlet 525-5, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations in the Strategic Army of the Early Twenty-first Century*, August 1994; Headquarters, Department of the Army; *FM 100-6, Information Operations*, August, 1996; Stuart E. Johnson and Martin C. Libicki, eds., *Dominant Battlespace Knowledge*, Washington, DC: Institute for National Security Studies, National Defense University Press, 1995.

19. "Brass Hats Get Down to Brass Tacks," *The Guardian*, May 24, 1997; Barry D. Watts, *Clausewitzian Friction and Future War*, McNair Papers, No. 52, Washington, DC: Institute for National Security Studies, National Defense University, 1996, pp. 3, 125; Dean A. Nowowiejski, *Concepts of Information Warfare in Practice: General George S. Patton and the Third Army Information Service*, Ft. Belvoir, VA: Defense Technical Information Center, 1996, pp. 2-3; Admiral William Owens, "Foreword," *The Information Revolution and National Security: Dimensions and Directions*, Stuart J.D. Schwarzstein, ed., Washington, DC: Center for Strategic and Information Studies, 1996, p. xii. Nowowiejski, pp. 2-3, 40; "The Information edge," pp. 44-47; Owens and Nye, pp. 20-36.

21. *QDR*, pp. 16-17; *NMS*.

22. *Ibid*.; United States Department of the Army, *Army Vision 2010,* Washington, DC, U.S. Government Printing Office, 1997; *QDR*, pp. 16-17; *FM 100-5*, pp. I, 4-5, II-0, II-6.

23. John J. Fialka, *War By Other Means: Economic Espionage in America*, New York, NY: W.W. Norton, 1997, pp. 110-111.

24. Toffler and Toffler, p. 67.

25. *Ibid.*, pp. 165-175, "TV Marti Seen as Example of New "Electronic Warfare," *Joint Publications Research Service, Soviet International Affairs*, June 5, 1990, pp. 33-35, cited in Stephen J. Blank, "Changing Missions for Soviet Space, Air, and Naval Forces," *Defense Analysis*, Vol. VII, No. 2-3, 1991, pp. 255-256.

26. For a revealing sign of the debate on this topic, see *Summary Report From the Conference on Preparing Now: Alternative Paths to Military Capabilities for an Uncertain Future*, Cambridge, MA: Institute for Foreign Policy Analysis, 1998.

27. FitzSimonds' remarks are in *Beyond the Technological Frontiers of Force XXI, Final Proceedings of an Army After Next Project Conference*, Atlanta, GA: Georgia Institute of Technology, Center for International Strategy, Technology, and Policy, 1996, pp. 9-10.

28. *Ibid.*

29. Interview of General Aharon Levran by Dr. Aaron Lerner, Director, Independent Media Review & Analysis (IMRA), December 14, 1997, *IMRA@netvision.net.il,* December 15, 1997. See also Allan Castle, *Transnational Organized Crime and International Security*, Working Paper No. 19, Institute of International Relations, University of British Columbia, Vancouver, BC, Canada, 1997, p. 10.

30. Ehud Ya'ari, "The Lebanon Surrender," *Jerusalem Report*, April 2, 1998, p. 25.

31. K. Subrahmanyam, "Covert Operations Pose New Challenges for Indian Security: In Search of Security After the Cold War," *World Affairs,* (New Delhi), Vol. I, No. 4, October-December, 1997, pp. 38-43.

32. *Ibid.*

33. *Ibid.*

34. *NMS,* p. 2, of section titled "The Strategy—Shape, Respond, Prepare Now."

35. *Joint Vision 2010*.

36. Richard J. Newman, "Can Peacekeepers Make War?" *U.S. News & World Report*, January 14, 1998, pp. 38-41; Bradley Graham, "U.S. Military Feels Strain of Buildup," *The Washington Post*, February 5, 1998, p. 6.

37. Williamson Murray, "Air War in the Gulf: The Limits of Air Power," *Strategic Review*, Vol. XXVI, No. 1, Winter, 1998, pp. 28-37; Timothy L. Thomas, "Air Operations in Low Intensity Conflict, The Case of Chechnya," *Airpower Journal*, Vol. XI, No. 4, Winter, 1997, pp. 51-59.

38. Fialka, pp. 101-105; Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica, CA: Rand Corporation, 1996, pp. 19-33.

39. *Ibid.*

40. *Ibid*.

41. At this internationally televised teach-in, student protesters and public opposition made it clear that the Secretaries of State and Defense as well as the Secretary of the National Security Council could neither offer a compelling strategic rationale for military action against Iraq nor gain popular support for it.

42. Robert Bunker, "Epochal Change: War over Social and Political Organization," *Parameters*, Vol. XXVII, No. 2, Summer, 1997, pp. 16-18.

43. "Osnovnye Polozhenii Voennoi Doktriny Rossiiskoi Federatsii," *Rossiyskie Vesti*, in Russian, November 19, 1993, *Foreign Broadcast Information Service Central Eurasia* (henceforth *FBIS-SOV)*-93-222-S, November 19, 1993, pp. 1-11; Colonel General I.D. Sergeev, "Improving Combat Readiness of Strategic Rocket Forces Under Conditions of Implementation of Strategic Offensive Weapons Treaties," *Voennaya Mysl'*, No. 6, November-December, 1995, pp. 16-21; Lieutenant General N. Ye. Solovtsov and Major General V.T. Nosov, "The Role and Place of Strategic Rocket Forces in Russia's Armed Forces," *Voyennaya Mysl'*, No. 11-12, November-December, 1994, pp. 71-76; Moscow, *Krasnaya Zvezda*, in Russian, March 13, 1998, *Foreign Broadcast Information Service Central Eurasia, Military Affairs* (henceforth *FBIS-UMA*)-98-075, March 17, 1998; Moscow, *Nezavisimaya Gazeta*, in Russian, January 22, 1997, *FBIS-SOV*-97-015, January 24, 1997;

Andrei Kokoshin, "Reflections on Russia's Past, Present, and Future," *Strengthening Democratic Institutions Project*, Kennedy School of Government, Harvard University, June, 1997, p. 31; Colonel V. Kruglov and Colonel M. Ye. Sosnovskiy, "Role of Nonstrategic Nuclear Weapons in Nuclear Deterrence," *Voennaya Mysl'* (Military Thought), No. 6, 1997, pp. 12-16; Moscow, *Voprosy Bezopasnosti*, in Russian, December, 1997, *FBIS SOV*, 98-064, March 5, 1998; Anton Surikov, "Some Aspects of Russian Military Reform," *European Security*, Vol. VI, No. 3, Autumn, 1997, pp. 49-65; Andrei Kokoshin, "Reforming Russia's Armed Forces, *Voyennaya Mysl'*, No. 5/6, 1996, p. 18; Lieutenant General (Retired) Ye. B. Volkov, "Start II and the Security of Russia," *Voennaya Mysl'*, No. 1, January-February, 1996, pp. 17-21; Major General V.A. Ryaboshapko (Retired), "Nuclear Conditions: Conditions of Possible Resort to Nuclear Weapons," *Voyennaya Mysl'*, No. 4, July-August, 1996, pp. 10-14; Colonel O.A. Kobelev and N.N. Detinov, "Upgrading the Nuclear Arms Proliferation Control System, *Voennaya Mysl'*, No. 9-10, September-October, 1994, p. 3; Sevastopol *Flag Rodiny*, in Russian, December 10, 1997, *FBIS-SOV*-98-009, January 12, 1998; Moscow, *Itogi,* in Russian, December 16, 1997, *FBIS-SOV*-98-020, January 23, 1998; Stephen Blank, "Russia, Ukraine, and European Security," *European Security*, Vol. III, No. 1, Spring, 1994, pp. 192-198; Mary Fitzgerald, "The Russian Shift Toward Nuclear War-Waging," *Hudson Institute*, Washington, DC, 1993. All the foregoing sources illustrate how Moscow sees both tactical and strategic nuclear weapons as weapons to be used to deter or counter purely conventional attacks and as weapons that could actually be used for warfighting purposes, i.e., as merely larger conventional weapons for use in conventional scenarios.

44. Molander, Riddile, and Wilson, pp. 19-33; David L. Marcus, "Nuclear Scenario Alarming to Think Tank," *Boston Globe*, March 21, 1998, p. 3.

45. See the sources cited in note 43. We should bear in mind George and Meredith Friedman's insight that nuclear strikes must be the opening move in a war, not the last one; hence the temptation to go first, even preempt, is very strong. Friedman and Friedman, p. 79.

46. Stephen J. Cimbala, "Russia's Nuclear Drawdown: Justice Delayed or Denied?" *European Security*, Vol. VI, No. 3, Autumn 1997, p. 81.

47. Watts, pp. 60-63.

48. Robert David Steele, "Private Enterprise Intelligence: Its Potential Contribution to National Security," *Intelligence and National Security*, Vol. X, No. 4, October, 1995, pp. 215-216.

49. *Ibid.*, p. 214.

50. Abraham Ben-Zvi, "The Dynamics of Surprise: The Defender's Perspective," *Intelligence and National Security*, Vol. XII, No. 4, October 1997, pp. 113-144.

51. Molander, Riddile, and Wilson, pp. 19-20.

52. *Ibid.*, pp. 21-33.

53. *Pravda Pyat 5*, in Russian, January 30-February 6, 1998, *Foreign Broadcast Information Service Central Eurasia* (henceforth *FBIS SOV)*-98-084, March 25, 1998; Moscow, *Segodnya*, in Russian, February 5, 1998, *FBIS-UMA*-98-036 February 5, 1998; David Hoffman, "Decline of Russia's Nuclear Forces," *The Washington Post*, March 15, 1998, p. 1; Bruce Blair, *The Logic of Accidental Nuclear War*, Washington, DC: Brookings Institution Press, 1993; and Bruce Blair, *Global Zero Alert for Nuclear Forces*, Washington, DC: Brookings Institution Press, 1995, pp. 18-23, 43-72. See also interview with John Newhouse, *Europe Adrift*, New York, Pantheon Books, 1997, pp. 211-212; and Pry, *War Scare*.

54. *Ibid.*, and see note 43.

55. *Ibid.*

56. Office of the Secretary of Defense, *Proliferation: Threat and Response*, Washington, DC: U.S. Government Printing Office, 1997, p. 44; D.L. Averre, "The Mirzoyanov Affair: Russia's 'Military-chemical' Complex," *European Security*, Vol. IV, No. 2, Summer 1995, pp. 273-305; Ken Alibekov, "Russia's Deadly Expertise," *New York Times*, March 27, 1998; Richard Preston, "Annals of Warfare: The Bioweaponeers," *The New Yorker*, March 9, 1998, pp. 52-65; Milton Leitenberg, "Biological Weapons Arms Control," *Contemporary Security Policy*, Vol. XVII, No. 1, April, 1996, pp. 1-79.

57. See note 43.

58. Cimbala, p. 76.

59. *Ibid.,* p. 79; Moscow, *Rossiyskaya Gazeta*, in Russian, September 23, 1995, *FBIS-SOV-95-188*, September 28, 1995, pp. 19-22; Dmitry Volsky, "The Explosive Karabakh Conflict," *New Times*, No. 16, 1993, p. 24; J.D. Crouch II, *et. al.*, "The Politics of Reform in Russia," *Global Affairs*, Vol. VII, No. 3, Summer 1993, p. 197.

60. John T. Fishel, *Civil Military Operations in the New World*, Westport, CT: Greenwood Publishing Group, 1997, p. 7.

61. *Ibid.* pp. 58-61, 100-103.

62. *Ibid*., pp. 241-242.

63. Jim Hoagland, "Victory Revisited," *Washington Post*, March 12, 1998, p. 15.

64. See the new National Security Blueprint, Moscow, *Rossiyskaya Gazeta*, in Russian, December 26, 1997, *FBIS-SOV*-97-364, December 30, 1997.

65. Lester W. Grau and Timothy L. Thomas, "A Russian View of Future War: Theory and Direction," *Journal of Slavic Military Studies*, Vol. IX, No. 3, September, 1996, pp. 501-518; Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters*, Vol. XXV, No. 4, Winter, 1996-97, pp. 81-91; Timothy L. Thomas, "Russian Views on Information-Based Warfare," *Airpower Journal*, Special Issue, 1996, pp. 25-35; Timothy L. Thomas, "Dialectical Versus Empirical Thinking: The Key elements of the Russian Understanding of Information Operations," Paper Presented to the U.S. Army War College, Annual Strategy Conference, April 22-24, 1997, Carlisle Barracks, PA.

66. Moscow, *Armeyskiy Sbornik*, September, 1996, *FBIS-UMA*-96-241-S, September 1, 1996; Colonel E.G. Korotchenko, "Informatsionno-Psikhologicheskoe Protivoborstvo v Sovremennykh Usloviakh," *Voennaya Mysl'*, No. 1, January-February, 1996, pp. 22-28.

67. *FBIS-UMA*, September 1, 1996.

68. "Russia's National Interests," *Obshchaya Gazeta*, August 14, 1997, from *Johnson's Russia List, djohnson@cdi.org*.

69. Andrei Piontkovsky, "Power Talk a Shameless Business," *St. Petersburg Times*, August 11-17, 1997, from *Johnson's Russia List*, *djohnson@cdi.org*.

70. Owens and Nye, pp. 20-36.

71. Timothy L. Thomas, "The Mind Has No Firewall," *Parameters*, Vol. XXVIII, No. 1, Spring, 1998, pp. 84-92.

72. Watts, pp. 43-68, 125-132.

73. *Ibid*.

74. *Ibid*., p. 8

75. *Ibid*., pp. 43-53.

76. James Kraska, "The Uninhabited Future of Military Operations," *National Security Studies Quarterly*, Vol. IV, No. 1, Winter, 1998, pp. 85-90

77. Molander, Riddile, and Wilson, pp. 21-33; Fialka, pp. 101-105.

78. Molander, Riddile, and Wilson, pp. 21-33.

79. *Ibid.*, pp. 28-29.

80. Frederick W. Kagan, "High-Tech: The Future Face of War? A Debate," *Commentary*, Vol. CV, No. 1, January, 1998, pp. 31-32.

81. Michael Brenner, "The United States," Michael Brenner, ed., *NATO and Collective Security*, New York: St. Martin's Press, 1997, pp. 162-175; *U.S. Civil-Military Relations: In Crisis or Transition?*, Don M. Snider and Miranda A. Carlton-Carew, eds., Washington, DC: Center for Strategic and International Studies, 1995; Deborah D. Avant, "Are the Reluctant Warriors Out of Control? Why the U.S. Military Is Averse To Responding to Post-Cold War Low-Level Threats," *Security Studies*, Vol. VI, No. 2, Winter 1996-97, pp. 59, 63, 86-89.

82. *Ibid.*

83. Bob Herbert, "War Games," *New York Times*, February 23, 1998, p. E17.

84. This observation is based on playing the U.S. Army War College's annual Strategic Crisis Exercise from 1995 to 1998 and the Army After Next Spring game in 1998, where coalition formation and maintenance invariably broke down or were often not even seriously attempted by the uniformed U.S. military. See also Brenner, pp. 162-175.

85. Herbert, p. E17.

86. Daniel Warner, "In Search of Security After the Cold War: US Security Concerns," *World Affairs* (New Delhi), Vol. I, No. 4, October-December 1997, p. 66.

REGIONAL STATE COMPETITORS: THE CASE OF IRAQ

Stephen C. Pelletiere

In any asymmetrical test of power, it is usually the case that the clash has been initiated by the stronger party. When the reverse occurs, that is bound to be of interest and worth investigating. In February 1998 Iraq took on the world's only superpower, the United States, and—expectations to the contrary—bested it. [1] I want to look at how Iraq achieved this feat. There should be some lessons here for the United States to consider. I propose to suggest a few.

Background.

Iraq had long ago decided that the inspections being carried on by the U.N. inspection teams were going nowhere. The *modus operandi* of the teams (in Iraq's view) was to poke into sites around the country, and, finding nothing, announce that the results were inconclusive.[2] This would necessitate the teams' returning at a later date. If this went on, the Iraqis reasoned, the inspections would never be finished, the sanctions would never be lifted, and the Iraqi people would go on suffering.

Sometime in 1997 (I don't think anyone but the inner circle of the Iraqi leadership knows exactly when) the leaders decided to call a halt, and thus in October 1997 Iraq's President Saddam Hussein announced that he would cease to cooperate with the weapons discovery effort, because, he said, it was being manipulated by the United States.[3] At that, the United States prepared for a confrontation. It let it be known that it would insist on Iraqi compliance, otherwise the Baathists could expect to be severely punished. As a spokesmen for the Administration

in Washington put it, "This time there will be no pin pricks."[4]

That was the setting in December 1997 as America prepared to go to war. And yet, as we all know, no war came. The Iraqis led the United States up to the brink, and then pulled back. After the fact, some pundits professed to believe that the Iraqis had lost in the test of nerves because in the end they did agree to resume cooperation.[5]

But for anyone who was following the episode at all closely, it is hard to make it out this way. To appreciate the scope of America's defeat, one must pay attention to events that led up to the eventual standdown. The devil is in the details, so to speak.

Prelude to Breakdown.

First off, America was abandoned in the confrontation by practically every one of her coalition partners.[6] Only a relatively few states stood fast. The rest (and particularly this was the case with three of the Security Council members—Russia, China, and France) dissociated themselves from taking military action. As if this were not bad enough, all of America's Arab allies (with the exception of Kuwait) abandoned it. Most striking was the defection of Saudi Arabia and Egypt.[7] Turkey refused to support the operation.[8] While not an Arab state, Turkey is an important player in the Middle East, and one whose support America has come to count upon.

It seems to me that none of the defections came about accidentally—Iraq set every one of them up. Baghdad planned the confrontation with the expectation that it would be possible to isolate the United States; and it did. How did it do it?

Manipulating Counters.

Iraq manipulated strategic and political counters. For example, Baghdad played on apparent contradictions in

America's great power role. On the one hand, the United States is the leader of the New World Order. Whereas in the past it led the fight against communism, now it claims to be the bastion of stability, the mainstay of the world economic system, the entity that facilitates the smooth running of the global system so that all of its operations mesh. That role, as presented, is eminently positive.

However, at the same time, America *is* a power, in the most primitive, brutal sense of the term. Nothing like its strength has been seen in history. And moreover that strength can be quantified, in actual numbers of weapons possessed. Power like this is intimidating. Lesser powers fear that the hegemon will throw its weight around.

This is the contradiction that Iraq played upon. It harped on the theme that America was in the Gulf—not, as the United States declared, to preserve stability, but to maintain the area as its personal sphere of economic and political influence. There was to be no activity carried on in the Gulf of which the United States did not approve. This specifically applied to trade relations. In the case of Iraq, Washington embargoed all trade; as to Iran, specific types of trade were interdicted. Why, the Iraqis asked, should the United States be able to set the terms of trade of nations like Russia, China, or France?

Iraq encouraged these and other states to trade with it. It let lucrative oil contracts, against the day when the embargo would be lifted.[9] Many states responded to Iraq's overtures, and grabbed at the opportunities held out. This gave them a vested interest in seeing the sanctions lifted. From there, it was small step to working to get them so.

That is how Iraq behaved with influential states in the United Nations. It behaved similarly with the Arab members of the coalition. Here, Baghdad manipulated the theme of the double standard. Why, asked Iraq, is Israel allowed to defy the United Nations with impunity, when Arab Iraq is castigated for conduct that really is not so bad? For example, Israel has an estimated 200 atomic bombs;

Iraq has none.[10] But the United Nations is embargoing Iraq on the chance that it might have some. Israel is occupying the territory of its neighbor, Lebanon, and has been since 1978, but the United Nations has allowed this occupation to go on.[11] Why? Because—according to the Iraqis—the United States defends Israel and supports its trespasses, at the same time that it requires the United Nations to deal harshly with Iraq.

This theme of the double standard resonates with the moderate Arab leaders—not because they are perturbed by the seeming illogicality of America's position, but because most of these regimes are basically unstable. They do not have an easy relationship with their people. Some states are only barely legitimate. The double standard theme, properly wielded, works on the Arab street to turn the people against the rulers. Indeed, worked on long enough and skillfully enough, it could bring down more than one of these regimes.[12]

As a longtime observer of events in the Middle East, I found it fascinating to watch how the double standard theme played out in this latest crisis. Towards the end of the affair—as Iraq and the United States were preparing to go to war—the moderate Arab rulers practically pleaded with the Iraqis to *give in*; *do not force a confrontation over this—let it lie*, *please!*[13]

Why were they so supplicatory? Because what Iraq was doing compromised them, fundamentally. In the streets—as the demonstrations started gearing up—Iraq was portrayed as the courageous party, standing up to Western imperialism and Zionism; while—by implication—the moderate Arab leaders were traitors who, by failing to come out in support of Iraq, actually were supporting the enemy.[14]

As a consequence, with open hostilities about to break out, America found that it practically could not get into the region. Almost without its being aware, America had lost its access to the Gulf. Not because the Iraqis barred the way,

but because moderate Arab regimes—fearful of a popular backlash—refused permission to use their bases for combat missions, and in some cases even denied overflight permission.[15]

This, I submit, represented the nadir of American involvement in this part of the world. At no time that I can think of has America's influence dipped so low. And, I contend, we were brought to this unhappy impasse by clever Iraqi maneuvering. The Iraqis so structured the situation that America could not exploit its greatest advantage, its vastly superior military power.

Of course, Washington *could* have used it. It could have gone ahead and attacked without coalition support. But this, in my view, would have been a very dangerous thing to have done. In the first place it would have put enormous strains on America's military, but, along with that, it would have deprived the nation of the moral basis that it needed for an operation like this. How could Washington claim to be acting in the interests of the international community, when practically the whole of the community had abandoned it?

Now what lessons can we draw from the affair?

Lessons.

The first lesson, obviously, is to take care of coalitions. In this particular crisis, coalition-building was not something that it was just good to do; it was essential. The Iraqi leaders saw that America's center of gravity was the coalition, and then set about to dismantle it. In doing so, they proved themselves to be good Clausewitzians.

At the same time, the Iraqis were aided by the Washington policymakers, who seemed incapable of assessing the danger—despite the fact that the Iraqis had practically telegraphed the strategy they would use. In November of 1996, they conducted what amounted to a trial run of the February 1998 showdown. I refer to their

operation in Irbil, where they came to the aid of the beleaguered Kurdish Democratic Party (KDP), being assaulted by the Iranians and their client the Patriotic Union of Kurdistan (PUK).[16] In the 1996 affair the Gulf sheikhs abandoned Washington, giving reasons similar to those expressed in February 1998. The same was the case with France; it stood aside on both occasions, justifying its behavior in practically identical terms.

Despite this warning, in February 1998 U.S. policy-makers behaved—right up to the end—as if the coalition would hold together.[17] It did not. When Saddam Hussein threw down the gauntlet a second time, America found itself constrained—actually, physically constrained. It could put its forces into the Gulf, but, once there, their maneuver room was limited. What was wanted was a substantial, land-based platform from which to launch, and that was denied it.

The lesson here, then, is that coalitions once struck must be maintained. The coalition partners must be regularly consulted to test their commitment, and if there is the slightest disaffection, this must be overcome.

Now for the second lesson—in any operation where the U.S. military might is employed, homefront support must be assured well in advance of the launch date. This is particularly so when (as happened in February 1998) the offending state shows an evident intention not only to stand up to a military trial, but an intention to survive the initial clash and force the issue.[18]

Iraq is a complex society. The regime there is largely misunderstood in the West. Western intelligence tends to emphasize the thuggish aspects of Baathist rule; and, it is true, the regime is ruthless. But it also is extremely well organized; its security apparatus extends throughout the society, and, as a consequence of this, the regime can count on considerable popular support.

In the February 1998 test, Hussein declared he would absorb whatever punishment Washington intended to inflict, on the assumption that his people would prove equal to the test. Afterwards, in the lull which would inevitably succeed the initial strikes, he planned to renew his challenge. By that time, he reasoned, world public opinion would have come over to his side—*he* would be seen as the victim and *Washington* the bully. Hence, it might be difficult for the United States to resume its assault.

Hussein's strategy may have been crafted for world consumption; in fact, however, it was likely to have had its greatest impact in the United States. Americans dislike being cast in the role of world policemen, and will submit to such a role only if individual "police actions" are easily gotten over with. An action such as Hussein planned, which was bound to drag out, would practically mandate an appeal by President Clinton to the American public for support—if not sacrifice. One can only wonder whether that would have been forthcoming.

If one looks at what occurred at Ohio State, there is cause for concern. There we witnessed the spectacle of three members of Mr. Clinton's cabinet trying to defend his Gulf strategy against a hostile audience.[19] One can say that Ohio State was a blip, that it revealed nothing of the true state of American attitudes. I think this would be a mistake. I suspect that the behavior of the dissidents betokened a profound unease felt by many Americans.

Most distressing about this episode was the character of the attack mounted against the hapless officials. To be sure there were unruly elements in the crowd, but there was also a lot of cogent questioning. And many questions, which ought to have been easily disposed of, either went unanswered or the replies proved unsatisfactory.[20]

Given everything that went on, clearly there was a need for good public relations to prepare the public for a sharp—possibly costly—engagement. That PR should have been well thought out and deftly handled. As the affair at

Ohio State showed, an element of the population is knowledgeable about world affairs and is sufficiently articulate to demolish glib defenses.

Finally, lesson three—perhaps the most important of all—which has to do with timing. It seems to me that, in the February 1998 confrontation, Iraq took advantage of the Asian meltdown. Financial conditions in the Far East began to unravel about the time that Hussein issued his ultimatum to the United Nations. As the Middle East embroglio escalated, Asia's situation became dire. The world looked to Washington to calm the financial turmoil in the Far East, but instead America prepared for war in the Middle East. This, of course, only increased the jittery condition of the markets.

I don't suggest that the Iraqis timed their challenge to coincide with the meltdown; obviously, they could not have done so. However, the Iraqis did nothing to mitigate the effects of their action; they went on apparently oblivious to the system-threatening aspects of what they were doing. Whereas another state might have pulled back, knowing that the system was endangered, the Iraqis apparently gave this no thought. *They may even have wished to cause a wreck.* Given the situation the regime found itself in, a meltdown probably would have had little effect upon it. Why?

Iraq is a pariah stae. And what does that mean? It means to be shut out of the system, not considered a part of it. The system, as we know, is economically oriented. Thus, a state that is excluded is denied access to capital. Not only can it not get any, if it has some it must hold on to it, since investment possibilities—for the pariah—are virtually non-existent.

Thus Iraq, having no stake in the world financial system, did not a care what might happen as a result of last February's confrontation. The system could come crashing down in ruin, and the Iraqis would not care. I believe something similar went on with Suharto and the Indonesia

crisis. There, too, an outcast leader played a spoiler's role. In Suharto's case, he too plunged recklessly on, ignoring International Monetary Fund (IMF) injunctions to amend his behavior, probably in the belief he could get away with it. Yugoslavia's Slobovan Milosevic's behavior over Kosovo may be another instance of this sort of risk-taking.

We must consider then that the true bandits of the world (those who have been cast so far out of the system they practically have lost touch with it) can, if they are sufficiently cold-blooded, wreak enormous damage. One could speculate that it was this perception of Iraq's damage-potential that persuaded American policymakers to let U.N. Secretary General Kofi Annan try to defuse the crisis before it got violently out of hand.

In an asymmetrical contest, look out for conditions the pariah can exploit—and, indeed, which are peculiarly suited to his advantage. As a pariah, he—like Samson pulling down the temple—has nothing to lose.

Now before I wrap this up I want to take up one last point—could this happen again?

Forcing the Issue.

I do not think there is any question about it. It not only can, but it will happen. Iraq sees the U. N. inspections crisis as one of national survival. It is determined to get out from under the sanctions, and the Iraqi people (because of the peculiar nature of the society) will go along with whatever step the leadership takes, no matter how apocalyptic.

Hence, this is not a crisis that is going to go away. Moreover, unfortunately for us, it is not a one-on-one affair, us against the Iraqis. (Were it so, I think our chances of imposing our will would be good.) Quite the contrary, in order to obtain closure, the United States must advance step-by-step with its coalition partners, and avoid doing anything that might dispose them to defect.

This is an almost impossible task. In two areas, U.S. policy has embarked on a course that is certain to offend the very states on which it must depend. The first involves trading with the Iranians—there, Washington's insistence that this not be done has alienated much of Europe. Moreover, it happens that two of the European states, France and Russia, currently are involved in a major deal with Tehran. I am referring to the effort by the French oil company Total (in conjunction with Russia and Malaysia) to exploit an Iranian gas field. President Clinton is seeking to finesse this confrontation, but it is not at all certain Congress will go along. In the meantime the Europeans have elevated the Total controversy to the status of a test case—if America remains intransigent, the Europeans have made it plain they intend to retaliate. In any case, we should not expect our European allies to support us in our next showdown in the Gulf.[21]

The second area in which problems are bound to arise is over the Arab-Israeli peace talks. Washington has shown it is dubious about going to the mat with the Israelis on this issue, which the Arabs feel it must do if the talks are to survive and bear enduring fruit. I do not believe that the administration has the will to force the issue with Israel. Consequently, the Arabs will remain disaffected, and they will not be on board when the next confrontation materializes.

The test almost certainly will come in October 1998 and possible sooner.[22] When it develops, we will be no better positioned to meet Iraq than we are today.

Overall, as I see it, the prognosis is bad; America is heading into a lose-lose situation. Is there anything it can do by way of extricating itself from this impasse?

Recommendation.

I think there is. But first off we must take a hard look at what is that we are dealing with here.

What we attempted to launch in February 1998—and are contemplating repeating at some future date—is a Military Action in the Absence of Threat (MAAT). That is my peculiar coinage; it is my way of referring to what I believe is a distinct class of operations. These are actions which—no matter how necessary they may be—are not perceived to be so by the public; rather the public views them as supererogatory.

As a consequence, such operations entail considerable risk. The officers conducting them have little margin for error, and should anything go drastically wrong they will find that the public has withdrawn support. As in the case of Somalia, demands will be voiced to bring the troops home. I think the Israeli experience in Lebanon is a good instance of this. It seems the ragtag Hezbollah militia is on the point of driving the mighty Israeli Defense Forces (IDF) out of Lebanon's southern region. The reason for this, primarily, is that the Israeli leadership has not persuaded the Israeli public there is a reason for staying on.

It is beyond the scope of this article to explain why America's leaders have failed to justify our military venture against the Iraqis. But it does seem to be the case that they have not. That, and the wholesale desertion by America's allies, betoken the unacceptability of the mission.

My advice, then, would be to avoid the looming confrontation with Iraq. We should do as former Defense Secretary Casper Weinberger did in Lebanon in the 1980s—withdraw, regroup and rethink our involvement. A good place to start would be with our assessment of the enemy, Baghdad. It seems to me we are ill informed on such basics as the nature of the leadership there, the relation of the leaders to the Iraqi public, and the place of a state like Iraq in the overall world system.

I think ignorance on that last point is part of what led us to concoct the truly, in my view, disastrous Dual Containment strategy whereby we set out to isolate both Iraq and Iran. That strategy has failed. The events of

February 1998 proved it so. We should use this experience as the basis for initiating a thoroughgoing examination of how Dual Containment should be revised, if it should not be totally abandoned.[23]

ENDNOTES

1. "CIA scores showdown: Saddam 1, Clinton 0," *The Washington Times*, January 8, 1998.

2. *FBIS-NES-98-043*, "Iraq: Al-Jazirah TV Interviews 'Aziz on Crisis," February 12, 1998.

3. "Iraq Orders U.S. Out of Inspections," *The Washington Post*, October 30, 1997.

4. "U.S. Digs In for 'Long-Term' Struggle Over Iraq Arms," *The Washington Post*, November 26, 1997.

5. *The Economist* leader article for February 28, 1998.

6. "Oman May limit U.S. Presence," *The Defense News*, December 1, 1997; "US and UK isolated in squaring up to Saddam," *The Financial Times*, November 15/16 1997; "Americans fail to win consensus on military action," *The London Times*, November 12, 1997; "Arabs angry with U.S. over Iraq crisis," *The Philadelphia Inquirer*, November 14, 1997; "Gulf Alliance: A Falling out," *The York Times*, November 13, 1997; "U.S. Position Weakens in Iraqi Standoff," *The Wall Street* Journal, November 4, 1997.

7. "Egypt's Leader Warns of Anti-U.S. Ire," *The New York Times*, February 18, 1998.

8. "Turkey sees no benefit in confronting Saddam," *The Washington Times*, February 6, 1998.

9. "U.S. Position Weakens in Iraqi Standoff."

10. "Iraq Is One of Many With Doomsday Arsenal," *The Wall Street Journal*, February 18, 1998.

11. See "US 'terror tactics,'" *The London Times,* November 10, 1997.

12. "On the Record, Arab Leaders Oppose U.S. Attacks on Iraq," *The New York Times*, January 29, 1998.

13. "Albright Reassures Arab States Caught in Dilemma," *The Washington Post*, November 17, 1998; "Arabs Angry With U.S. for Iraq Crisis; "Gulf Alliance: A Falling Out."

14. See "Pro Iraqi West Bank Protests Blocked by Palestinian Police," *The New York Times*, February 10, 1998; "Hamas urges pro-Iraqi demonstrations," *The Philadelphia Inquirer*,, February 17, 1998; "Prospect of Military Action Draws Protest, *The Washington Post*, February 14, 1998.

15. See note 6.

16. Stephen Pelletiere, *Managing Strains in the Coalition: What to do About Saddam*? Carlisle, PA: Strategic Studies Institute, U.S. Army War College, November 1996.

17. "Cohen Finds Gulf Nations Hostile to Military Action," *The New York Times*, February 11, 1998.

18. "Baghdad's calculated gamble," *Middle East International*, November 21, 1997.

19. "Top Aides Shouted Down At 'Town Meeting' on Iraq," *The Washington Post*, February 19, 1998; "Hostile Responses Disrupt a Favored Clinton Forum," *The Washington Post*, February 19, 1998; "Town meeting gets rowdy," *The Patriot-News* (Harrisbug, PA), February 19, 1998.

20. "War of Words: The Administration, Its Critics and Questions of Moral Right," *The New York Times*, February 19, 1998. This is an excerpted version of the session at Ohio State.

21. "Avoiding total war," *The Financial Times*, October 3, 1997; "US pressed on Helms-Burton," *The Financial Times*, October 20, 1997; "Canadians in Iraq oil deal, *The Financial Times*, December 16, 1997; "US Rethinking Stance on Economic Sanctions," *The Washington Post*, January 26, 1998; "Demands for Oil Influence Policy in Gulf," *The Wall Street Journal*, February 23, 1998.

22. This is when the UNSCOM mandate will come up for renewal. But there were signs of resurrected defiance by Saddam Hussein as early as late April 1998.

23. F. Gregory Gause III, "The Illogic of Dual Containment," *Foreign Affairs,* No. 73, March/April 1994, pp. 56-57.

BEYOND RUSSIA AND CHINA: A SURVEY OF THREATS TO U.S. SECURITY FROM LESSER STATES

Kori N. Schake

Introduction.

This paper addresses state-to-state threats excluding Russia and China. It reviews challenges posed by the usual suspects—North Korea, Iran, and Iraq—none of which are considered to be major military challengers. It also identifies six functional areas of state-to-state threats that could diminish U.S. security or require rethinking our approach: (1) anti-U.S. coalitions; (2) contested emergence of new states; (3) regime change among existing allies; (4) inhibiting the use of U.S. forces; (5) critical dependence on allies; and (6) criminalization of governments.

The Usual Suspects.

The United States faces very little prospect of an attack, and our values are shared by more countries than ever before. The intelligence community has determined that a "peer competitor" to U.S. power is unlikely to emerge within 15 years. This makes rounding up the usual suspects more difficult than it used to be.

Russia and China have been ruled out of bounds for the purposes of this paper. Of the remaining possible regional challengers, Libya is probably no less implacably opposed to U.S. interests than previously, but has been so circumspect since the 1986 *El Dorado Canyon* raid as to barely merit mention.

Iraq. Iraq continues to be an irritant, but not a major military threat to U.S. interests in the Gulf. Iraq poses a more tangible state-to-state threat than either North Korea or Iran; however, the threat it poses is more of a political

than military nature. Iraqi military forces could not pose a serious challenge to a dedicated U.S. force even during the 1991 Gulf War, when they were in considerably better shape than now. The 7 years of operational and economic restraints imposed by the U.N. authorities have not permitted serious reconstitution of their forces.

Saddam Hussein's chemical, biological, and nuclear weapons programs remain cause for considerable concern, and could be used in attacks against military installations or civilian targets in the Middle East. However, the clear result would be targeting of the Iraqi regime by U.S. forces, so it is more likely that the weapons are to deter attacks on the regime than to conduct offensive or terrorist operations. While Iraq continues to require careful U.S. and international attention, it does not pose a major challenge to the United States.

North Korea. The state-to-state threat against which the United States has committed the most resources is aggression by North Korea against South Korea, possibly coupled with attacks on Japan and other regional U.S. allies. In the past few years, North Korea has massed its troops along the demilitarized zone, proliferated missile technology export to rogue regimes like Iran, sent a submarine load of special forces commandos into South Korean waters, and continued to fund a substantial nuclear weapons program. North Korea maintains the world's third largest chemical weapons inventory and, despite terrible economic deprivation, is building ballistic missiles with ranges from 600 through 6,000 miles.[1] In addition, the KIM Chong-il regime gives every indication of being aggressive and irrational. Distinguished experts in Asian security issues believe North Korea to be capable of a "suicidal gamble," attacking South Korea rather than fading from power under the weight of a failed economy and political system.[2] None of these are reassuring prospects for maintaining the status quo or achieving a peaceful unification of the Koreas.

However, there are significant signs that the Democratic People's Republic of Korea (DPRK) is moving toward a "soft landing" of gradual unification with the South rather than a violent implosion. All of North Korea's potential adversaries have been providing substantial aid during the past two years' famine, making them less likely targets of aggression.[3] China, Russia, Japan, South Korea, and the United States are all committed to managing North Korea's decline without provocation.[4] South Koreans have little desire to undertake the massive development task of rapid unification, especially after the Asian economic crisis.[5] The newly-elected South Korean government is more conciliatory toward the North, which may further ease tensions on the Korean peninsula.[6] The DPRK appears to be responding in positive ways to these developments; it recently offered to hold bilateral talks with the South Korean government in Geneva, demonstrating a greater interest than before in cooperation.[7]

Even if the DPRK wanted to attack South Korea, it is unlikely to have the ability to do so. North Korea is facing starvation on a scale so debilitating that it is unlikely to be able to put an army in the field.[8] While it is impossible to assess the motivating effect of North Korean propaganda, it is difficult to imagine troops who have starving families (even if they are not starving themselves) fighting an aggressive war waged by the DPRK. Any effort by the North Korean government to organize a conventional military assault on South Korea would probably result in large-scale defections and surrenders. In fact, the North Korean regime should be more concerned about troops turning their weapons against the government than against troops assembled on the southern side of the demilitarized zone—and the North Korean government must be well aware of that possibility.

The prospect of an unconventional "last-gasp" attack by a collapsing DPRK is a more serious threat.[9] Faced with the imminent crumbling of state authority, the North Korean government could probably motivate special forces units to

stage terrorist attacks throughout South Korea and in allied states.[10] These could take the form of a coordinated campaign of covert attacks intended to disable U.S. and South Korean military capabilities: chemical or nuclear attacks on airfields and other large military installations, interdicting communications lines, and assassinations of South Korean and American military leaders. A North Korean attack of this nature could also be directed at the South Korean political system, in which case the targets would be more punitive: assassinations of South Korean political leaders, poisoning water supplies, and directing nuclear weapons at Seoul and other large population centers.

The problem with a North Korean last-gasp attack scenario is discerning the purpose it would serve. If the regime were completely irrational, there is no reason to believe it would have waited this long to attack the South; what rational objective the DPRK could achieve in its current condition is unclear. The DPRK may hunger over the prospect of forcing the South into servitude, or acquiring the wealth and food enjoyed by South Koreans. But desperate military measures such as the last-gasp attack could not achieve those ends. Without the ability to take and hold territory, which only a disciplined army could provide, the North could not enjoy the advantages potentially stolen from the South.

Even if the North's motive were simply to punish the South, a last-gasp attack could only take South Korea down as the North sinks itself. The long-standing U.S. commitment to defense of South Korea and the impressive military capabilities assembled in the South make the consequences of any attack, military or paramilitary, abundantly clear. The United States would certainly retaliate for an attack on South Korea, and would probably target the DPRK regime rather than territory or even organized Northern military forces. It is possible that the last-gasp scenarios serve domestic purposes in North Korea, since the threat of launching such attacks serves the

interests of regime survival as circumstances in North Korea grow ever more desperate.[11]

Even if a coterie of the North's leadership were irrational enough to want to go out with a bang, it is quite possible that some in the political and military leadership would seek to stymie that effort. The election of a South Korean president more conciliatory toward the North, and himself a victim of repression by former South Korean regimes, makes a last-gasp attack even less likely. Some in the DPRK regime—paralleling decisions by some in Hitler's regime—could well consider their prospects more attractive in assisting the ROK government than in carrying out a suicidal last-gasp attack.

For all these reasons, North Korea is losing its credibility as a potential aggressor state. While the DPRK regime remains worrisome, its ability to threaten the South is diminishing. Tensions on the Korean peninsula appear to be dissipating as both Koreas become more conciliatory, and the DPRK teeters on the brink of economic collapse.

Iran. Iran is the final state generally conjured up as a usual suspect for attacks on U.S. interests by another state. It has emotional appeal as a villain because of the 1979 hostage crisis and the anti-Western revolutionary fervor of Ayatollah Khomeni and his successors. The Islamic Republic of Iran funds terrorist organizations, may well be embarked on a clandestine nuclear weapons program, is acquiring long-range ballistic missiles, opposes the Israeli-Palestinian peace process, makes America's regional allies nervous by challenging their support of U.S. military presence in the Gulf, and continues to enjoy the lather of its own anti-American rhetoric.[12] Since the Gulf War, Iran has been engaged in a substantial military buildup. It boasts the largest regional navy in the Gulf, substantial missile and mine capabilities, limited power projection capability, and a growing submarine force.[13] Iran probably already has the ability to threaten oil shipments through the Straits of Hormuz.[14]

Iran's ability to influence states in the Middle East appears limited to supporting terrorism. Religious differences inhibit Iranian influence beyond its borders, since Shi'i Muslims constitute only 15 percent of the world's Muslim population and most reside in Iran.[15] In the 19 years since the revolution, Iran has failed to become a model for other Islamic states, even in Iraq, which has a majority of Shi'i Muslims.[16] Arab states remain wary of Iran for promoting Islamic militancy. The end of the Cold War probably also diminished Iran's power by making Russian collaboration less commercially and politically profitable and, due to arms control agreements like the Missile Technology Control Regime, less militarily beneficial.[17]

Positive political developments in Iran in 1997 make the picture more conducive to U.S. interests and influence than it has been at any time since the 1979 revolution. In May of 1997, Iran's leaders acquiesced in election results that brought President Mohammed Khatemi to power with public support around 60 percent, even though he was not their preferred candidate. This may mark Iran as the most honestly democratic Islamic state in the Middle East.

At a December 1997 meeting of Gulf leaders, Ayatollah Khameni voiced the standard Iranian attacks on the United States and Israel, but President Khatemi took a much more moderate and cooperative line, even professing that Iran no longer would support covert operations against other governments.[18] There is some evidence that the Iranian military supports this more moderate approach.[19] In a January 1998 interview on CNN, President Khatemi even called for greater contact with the American people.[20] The widely divergent approaches of President Khatemi and Ayatollah Khameni suggest a power struggle within Iran's ruling circle. While Khameni holds most of the statutory authority for security and foreign policy, the breadth of support for Khatemi may sway Iran in the direction of greater common interests with the United States.[21]

Even before Khatemi's election, Iran may have adopted a more conciliatory policy toward America. Iran may have been attempting to signal a desire for improved relations with the United States as early as 1996, when Conoco was granted an oil development contract.[22] These developments clearly suggest that "dual containment" is no longer a useful strategy for the United States.[23] American interests would be better served by rewarding cooperative Iranian behavior than continuing the embargo.[24]

Nightmare Scenarios.

If not the time honored shibboleths of North Korea, Iran, or Iraq, what other state could pose a threat to the United States?

The possible conflicts to be adumbrated here are not likely prospects. Even if they were to become likely, the United States has many tools to shape events as they occur. But examining nightmare scenarios can nonetheless be useful, even when they are as unlikely as any state developing the ability to defeat the U.S. Army in the coming 15 years. Nightmare scenarios can probe for weaknesses in our forces or our decisionmaking practices that could be exploited by potential enemies. They can identify policies that limit or compensate for U.S. vulnerabilities. And they can suggest possibilities that straight-line extrapolations from present trends might miss.

I'd like to suggest six categories of state-to-state threats that could emerge as nightmare scenarios for the United States: (1) anti-U.S. coalitions; (2) violent emergence of new states based upon ethnic consolidation; (3) adverse regime change among existing allies; (4) enemy manipulations inhibiting the use of U.S. forces; (5) RMA-induced incompatibilities between U.S. forces and allies; and (6) criminalization of governments. I use examples to illustrate the arguments, but would like to emphasize that none are likely futures.

Anti-U.S. Coalitions. While no single state may pose a threat to the United States, it is relatively easy to imagine coalitions of states who could find common cause in opposing U.S. interests, even without bringing in Russia or China directly. While even in combination most countries could not defeat American forces, it is important to recall that states do not always have to achieve military success for military operations to successfully serve strategic purposes. The Egyptian invasion of Israel in 1973 demonstrated Israel's vulnerability, garnering an important political success for Anwar Sadat. The Iraqi invasion of Kuwait resulted in a resounding military defeat but may well have served Saddam Hussein's broader political purposes in the Arab world. It is not necessarily irrational for states to use force against U.S. interests even when they cannot conceivably defeat U.S. forces. Two examples of anti-U.S. coalitions that could serve the members' strategic interests are: a coalition of Iran and Iraq; and a coalition of the ailing Asian tigers.

While Iran and Iraq fought a costly 8-year war against each other, the "dual containment" policy provides them common cause. If sanctions against both countries were to cause widespread public deprivation or call the regimes into question, the two governments might eventually find reason to cooperate in attacks on U.S. forces in the region, or assist each other in eluding U.N. (in the case of Iraq) and International Atomic Energy Agency (in the case of Iran) inspections of their nuclear facilities.

This possibility could actually increase if Saddam Hussein were deposed. The paramount internal threat to the Iraqi regime emanates from Iraq's Shi'i, who constitute the majority of Iraq's population and oppose the regime.[25] If Iran, which is also predominantly Shi'i Muslim, actively supported Saddam Hussein's overthrow, a friendly Shi'i government could well come to power in Iraq.

Gulf allies might fear supporting the United States against an Iranian-Iraqi coalition, even if U.S. forces in

their territory are attacked, because of domestic unrest or fear of delegitimizing their own regimes.[26] The presence of U.S. military forces in the Gulf Cooperation Council (GCC) states could become "a lightning rod for domestic discontent."[27] Iran and Iraq could also team up in attacks on regional U.S. allies, several of whom (including Saudi Arabia) have aggrieved both Iran and Iraq.[28] There are such fractious divisions among the GCC states, so little security cooperation among them, and despite substantial arms procurements such little defense capability, that the combined military forces of Iran and Iraq could inflict substantial damage.[29] Collusion by either Russia, which still covets a Middle East role, or China, which is growing ever more dependent on Middle East oil as its economy develops, would further aggravate the U.S. position. Either Russia or China could stymie U.N. action, supply weapons and intelligence, and make unilateral U.S. action more costly. Such a coalition of Iran and Iraq, even if only temporary, would prove disastrous to U.S. interests in the Arab world.

Another anti-U.S. coalition of moment would be among the authoritarian Asian regimes. The economic crisis that Indonesia, Thailand, Singapore, and Malaysia are currently experiencing not only deflates the myth of invincible Asian tigers, it also constrains their sovereignty.[30] If economic restrictions required by the International Monetary Fund cause public resentment, governments could attempt to deflect criticism onto the IMF or the United States as the Fund's ideological center of gravity. Senior officials from the affected countries have already denounced American currency speculators, and anti-IMF sentiment has become a public rallying cry in Indonesia.

Forcing a level economic playing field will undercut the crony capitalism through which political allegiances have been cemented in several of the Asian states. The pains of the economic crisis are likely to hit urban poor the hardest, mobilizing the greatest threat to authoritarian govern-

ments.[31] If authoritarian leaders eventually decide this threatens their hold on power, they could turn against the United States in an effort to shield their economies and political systems from change. Even without cooperating with China or Russia, the Asian tigers could interdict shipping across the Straits of Malacca and other choke points in the Pacific. With sympathetic Chinese support of anti-American authoritarian regimes, Asia could look much less hospitable to U.S. interests.

Contested Emergence of New States. The Wilsonian ideal of state borders representing identifiable ethnic communities is coming into being, in many cases violently, now that Cold War restraints have been lifted. Ethnic communities in territorially cohesive regions pulled away from the Soviet Union to establish states in Latvia, Lithuania, Estonia, Azerbaijan, Georgia, Armenia, Tajikistan, Kazakhstan, Turkmenistan—and more may yet be coming from within Russia. States which have intermingled ethnicity and territory, like Bosnia, are at even higher risk of violent dissolution as new ethnically-based states are created. The emergence of new states has already instigated U.S. military involvement to prevent epidemic starvation and atrocities, while upholding humanitarian and democratic values.

In most cases, support to collapsing or emerging states is a luxury rather than a necessity for the United States. However, the emergence of two particular states could pose definite challenges to U.S. security interests: a Kurdish state across swaths of Turkey, Iran, Iraq and Syria; and an Albanian state cut out of Yugoslavia.

Iraq's borders do not cohere to ethnic or national boundaries; they were set by fiat in 1926. U.S. intervention to protect Kurds in northern Iraq after the Gulf war, now sustained for 7 years, has both fomented the idea of a Kurdish state and resulted in the *de facto* detachment of the territory occupied by Kurds from Iraq. Kurds also live in Iran, Syria, and Turkey—all of which oppose establishment

of a Kurdish state, even if it were composed solely of territory from Iraq.[32] While Iran and Syria sporadically support Kurds in Iraq, they do so on the basis of harming Iraq's government; Turkey supports Iraqi Kurds in return for their assistance in putting down the PKK Kurdish movement in Turkey. None of the three governments would accept any one of the others incorporating Kurdish territory from Iraq into their own states.

All of which suggests that if Iraq collapses, Turkey, Iran, and Syria will probably use military force to prevent each other from absorbing parts of Iraq. Turkey would almost certainly seek support from the United States if the territorial status quo were challenged by Iran or Syria. Denying such support would validate Turkish suspicions that its NATO allies do not appreciate the gravity of the "Kurdish problem" and cannot be counted on for support in a crisis, giving Turkey yet one more reason to turn away from the West. Providing support would damage U.S. relations with the Arab states, who view Turkey with suspicion, but who in any event would have a strong interest in supporting the retention of existing borders. Either way, the United States loses critical allies.

If Iraq begins to collapse, Turkey could also be the first state to use force, since its army is already operating in northern Iraq. It is in position to intervene and is already familiar with the terrain and patterns of operation by Kurdish factions in Iraq. There were suggestions during the Gulf War that Turkey might move quickly into northern Iraq to prevent Iran or Syria from gaining territory. If Turkey were the first state to challenge Iraq's territorial integrity, it would be even more difficult for the United States to support Turkish military action. Having fought Iraq to preserve the principle of territorial integrity, America would have a public relations nightmare explaining its support for a Turkish invasion of Iraq.

A second scenario detrimental to U.S. interests based on the emergence of a new state could occur in Yugoslavia.

Kosovo holds so powerful a position in the Serbian sense of identity that Serbian acceptance of Kosovo's independence is difficult to imagine. Ethnic Albanians constitute 90 percent of the population of the Yugoslav province of Kosovo, yet they have very little autonomy and virtually no political power.[33] Serbs living in Kosovo, with the support of the Milosevic regime in Belgrade, have constrained political and social freedoms for Albanians in Kosovo for the past 2 years, breeding radicalism among Albanian Kosovars.[34] Serb paramilitary forces have used force indiscriminately, killing dozens of people who do not appear to have been involved in illegal activities.[35]

The U.S. government has long considered violence in Kosovo to be the major potential flash point in the former Yugoslavia—the contingency that could bring two NATO allies (Greece and Turkey) into a war on opposite sides.[36] U.S. pressure for sanctions against Serbia met a cool response from Italy, France, Germany, and Russia; German Foreign Minister Klaus Kinkel has even suggested that the Serbian repression was legitimated by the actions of Albanian Kosovars. Signatories of the Dayton Peace Accords know that the success of NATO's mission in Bosnia depends on support of Yugoslav President Slobodan Milosevic for any hope of eventual success in pacifying Bosnia. Although both countries condemned violence in Kosovo, Turkey is sympathetic to Albanian Kosovars, Greece to Serbs.[37]

If the latest round of Serbian pressure creates more rather than less agitation for independence in Kosovo, subsequent rounds of negotiations could see a yawning gap between the positions of the United States and Turkey on one side and our major European allies along with Russia on the other. Albanian Kosovars may declare independence from Yugoslavia, challenging President Milosevic to defy Western warnings. If Serbia continues its repressive tactics in Kosovo, the Albanian majority may turn violently against Serbs living in the province, precipitating a destabilizing exodus of refugees to neighboring countries and even more

violent repression by Serbian military and paramilitary forces brought in to quell the disturbance.[38] An Albanian uprising supported by Turkey and other opponents of Serbia would quickly precipitate calls for an American military intervention, even though there would be very little public support for it in the United States.

An explosion of Kosovo would not only affect the Balkans, but Greece would almost certainly encourage European Union action against Turkey, aggravating disagreements over Cyprus and the status of Turkey's application for EU membership. The United States would be caught between its allegiance to Europe and its responsibility as the only country able to keep Turkey in the Western camp.[39] Even if Kosovo were able to overcome political and military challenges to its independence, the Balkans would have one more fragile, turbulent, economically marginal country with outsiders angling for influence.

Regime Change Among Existing Allies. The United States depends heavily on the support, both political and military, of regional allies in the conduct of our security policy. In many cases, and especially in the Middle East, the United States is supported by unstable or only marginally stable ruling regimes—-those with uneasy relationships with their populaces. A change of regime in any number of states allied to the United States, whether peaceful or violent, could have dramatic effects on our ability to successfully continue current security policies. A regime change in either Egypt or Saudi Arabia could have particularly devastating effects on U.S. interests.

Egypt is unlikely to "succumb to a reign of theocratic zeal," but the steady descent into poverty and hopelessness that has characterized Egyptian political life in the past decade could well have unpredictable results.[40] The economy is moribund and losing even its tourist cachet because of violence against foreigners intended to punish the government. The government of President Hosmi

Mubarak has cracked down on terrorist and dissident activity, but has not engendered an active and positive state role to balance its negative effects. In addition, Mubarak's acceptance of a third presidential term in 1993 created the prospect of an authoritarian Egypt with no orderly succession.[41]

It is difficult to imagine Egypt becoming an aggressor against its neighbors, but an escalation of domestic violence like that which occurred when President Anwar Sadat was assassinated is conceivable. An effort to overthrow the regime, especially if it were supported by Egyptian military units, could create an upheaval within Egypt. The United States would likely be called on to support the regime with military forces in the region.

A regime more focused on Egypt's domestic problems, even if not explicitly anti-American, would cost the United States a valuable partner in the Middle East peace process. A regime that challenged the Sadat and Mubarak governments' commitment to peace with Israel could have much more nefarious effects on U.S. interests. If an Egyptian government worked with Iran, Iraq, and other opponents of peace with Israel, the nature of political dialogue and U.S. calculations about the cost of support to Israel could change significantly.

A regime change in Saudi Arabia could also have deleterious effects on U.S. interests in the Middle East. Pressure is rising there for more representative and liberal government. While internal change is in both Saudi and U.S. interests, unless that change toward democracy is well managed, the Saudi government could be destabilized. The deployment of U.S. forces in GCC states strains the legitimacy of those regimes in the best of circumstances, but a virtual collapse of the Middle East peace process (particularly since many Arab publics ascribe its failure to Israeli intransigence) coupled with a seemingly personalized American crusade against Saddam Hussein that punishes the Iraqi people without removing Saddam,

will make GCC governments that support U.S. policies and forward deployments more vulnerable.

An economic downturn among the GCC states, similar to that currently being endured by Asian governments, would badly aggravate the problem. Oil prices plummeted 40 percent in the February-April 1998 timeframe, and 75 percent of the Saudi economy depends on oil.[43] While an unusually warm winter in 1997-98 and the Asian slowdown have contributed to the international oil glut, prices are also low because Saudi Arabia is producing oil in excess of OPEC guidelines—which suggests that the Saudi government is concerned about the effects of an economic downturn. Cuts in government subsidies could increase public unrest and diminish tolerance for the government's other unpopular policies. Even if the Saudi government were not toppled, concern about public unrest could lead to reticence in supporting U.S. positions that would impair U.S. ability to harness the Iraqi government, coax moderation from Iran, and sponsor peace negotiations between Israel and the Palestinian Authority.

Regime changes precipitated by domestic developments would be difficult scenarios for the United States to intervene in militarily. They require a sophisticated understanding of the societies that we rarely achieve and seldom provide opportunities for "clean" uses of force. However, if either the Mubarak government in Egypt or the Saudi government were in danger, they may well call for U.S. military assistance. If that assistance were not given, the United States could watch two of its most valued allies in the Middle East sink. If that assistance were given, it could result in our propping up a government lacking domestic legitimacy and thus requiring long-term constabulary commitments. It is difficult to think how with anything less than constabulary use of its forces, the United States could stave off regime change—resulting in the emergence of governments hostile to U.S. interests.

Manipulations Inhibiting the Use of U.S. Forces. States determined to oppose U.S. security policies need not fight the U.S. military if they are able to prevent the United States from fielding or employing our forces. One of the easiest ways for a state to achieve that goal would be to threaten retaliation against U.S. allies. For example, if the Iraqi government threatened to use chemical or biological weapons against Israel in response to an attack by U.S. forces, it would gravely increase the political and moral costs to the United States of attacking Iraq. It may not prevent an attack, but it would send U.S. decisionmakers searching for options. The actual use of chemical or biological weapons against Israel would probably strengthen U.S. resolve to use force, resulting in U.S. military forces directly targeting the regime rather than its military forces. But the simple threat of itself would raise the costs to the U.S. for using force.

A regime sophisticated enough to work on U.S. public and congressional anxieties about high casualties, mission creep, or long-term commitments of force could raise the price to the U.S. government of using force in the conduct of security policy. Once forces were deployed, sniper attacks, guerrilla tactics, and atrocities like torturing prisoners could also generate public pressure to end commitments of U.S. military force.

Threats against allies and demonstrating a determination to inflict sustained pain on the United States are ways that a state could defeat the U.S. military by preventing it from ever being employed or precipitating its premature withdrawal.

RMA-Induced Incompatibilities Between U.S. Forces and Allies. The United States is incorporating communications and other technologies into the equipment of its military in ways that are already changing our warfighting doctrine. Whether or not these changes constitute a "revolution in military affairs" (RMA), they are making our military forces different in important ways from

the forces of our friends and allies. U.S. forces are developing a battlefield awareness far superior to that of other militaries, giving us control that could result in far fewer casualties than would be risked by other nations. The great leap forward in technology could make it more difficult for the United States to build coalitions—other nations will not have the ability to contribute much to the kind of warfare our forces will be trained to conduct, and those that still contribute could face the prospect of being mere *fussvolk* with high casualty rates not suffered by the Americans.

One way out of this dilemma being discussed at NATO is increased mission specialization among allied forces. Mission specialization already occurs, as the United States realized during the Gulf War when it depended on European navies for much of the coalition minesweeping capability. But it could be extended over time to having allies responsible for things like strategic lift, theater reconnaissance, and other compartmented capabilities that would allow allies to materially contribute as peers to a U.S.-led coalition, even though they do not maintain the full range of capabilities in their forces. A mission specialization system would allow allies to target their defense spending in narrow slices of the spectrum so that they could afford high-end capabilities.

Such an approach would diminish Congressional burdensharing concerns. However, it could also create critical dependencies on allied forces if the United States does not maintain redundant capabilities. The end of the Cold War made it more difficult to predict the states that will join "coalitions of the willing." If U.S. forces become dependent on niche capabilities of other states' forces, the failure of a particular ally to support U.S.-led coalition operations could bring operations to a screeching halt. A savvy antagonist would ferret out those dependencies, identify the countries that hold the keys, and them exploit that vulnerability.

Criminalization of Governments. The gravest security problems for the United States would result from criminalization of Russia or Mexico. In either case, the rise of criminal influence over the government would make the United States vulnerable: in the case of Russia, because of the remaining nuclear arsenal; in the case of Mexico, because of its barely guarded 2,000-mile border with the United States. The most problematic scenario would involve retaining the forms of democratic governance without their substance, because that would make it more difficult for us to mobilize support for isolating the criminal regimes.

Organized crime has already reached worrisome proportions in Russia. The government in Moscow could be at risk of losing control, with the country reverting to feudal fiefdoms controlled by thugs. There are enough leaks in the Russian security system to make a true nightmare scenario believable: a Russian government cooperative with the West but lacking control of its nuclear forces; antagonists able to steal or buy cooperation from Russian regional, intelligence, or military leaders; and the Russian government not wanting to appear so weak as to need U.S. intervention in maintaining control over its own force. A Russian government grown disgruntled by its loss of stature, economic deprivation, and being taken advantage of by the West for its weakness would only aggravate the situation by making the Russians less cooperative in supporting our common interests.

Drug Czar Barry McCaffrey recently characterized Mexico as "fighting for its very life against drug lords." The Mexican government brought its military into law enforcement in 1996 because it was considered the least corrupt enforcement agency; but the arrest in 1997 of General Jesus Gutierrez Rebollo, the head of drug enforcement, demonstrated how quickly the military was compromised. A recent Drug Enforcement Agency (DEA) report suggests widespread collusion between the Mexican military and drug mafia.[45] The huge amount of bribe money drug cartels can provide to politicians and law enforce-

ment—on both sides of the 2,000-mile U.S.-Mexican border—allows the drug mafia to buy silence and acquiescence. The money also increasingly allows them to buy sophisticated intelligence systems, weaponry, and the expertise of former U.S. military personnel.

Aside from a Russian nuclear threat, U.S. loss of border control is the most direct threat to its security interests. Such a development would destabilize the southwest, one of the most vibrant economic and cultural regions of our country. It would exacerbate the social problems associated with drug abuse in the United States. It could make the nature of the U.S. immigration debate much more hostile. A public belief that their country had lost control of the border, coupled with substantial violence along it, would likely precipitate a call for redirecting U.S. defense efforts closer to home. Border defense and constabulary functions could become major U.S. military activities, changing both the nature of defense efforts and the military's relationship with our society.

A different but related threat would be delegitimation of the Mexican government. If Mexico were to become as penetrated by drug money as Colombia, its institutions would be unreliable.[46] The Juarez drug cartel has already breached Mexico's banking industry, although the Mexican government successfully identified the incursion.[47] Drug-related corruption and kidnapping are occurring in the top echelons of state law enforcement apparatuses throughout Mexico.[48] Delegitimation of Mexican governmental institutions would be compounded if Mexican citizens foment rebellion against the government in areas like Chiapas.

The increasing democratization of Mexico's political system diminishes the prospect sketched above somewhat, but the Mexican government will have to guard against outright purchase of legislative seats, keep police pressure on drug cartels, and better enfranchise its population in order to avoid the kinds of problems currently being

experienced by Colombia.[49] Moreover, Mexico's citizens will have to demand good government and police it with a free press.

Conclusion.

None of the state-centered threats identified in this paper are likely developments. A return to revolutionary fervor in Iran coupled with an Iranian-friendly regime in Iraq; a coalition of authoritarian Asian states building common cause against international financial institutions; the collapse of Iraq with subsequent involvement by Syria, Iran, and Turkey to prevent emergence of a Kurdish state; regime change by internal revolt in Egypt or the GCC states; and criminalization of Russia or Mexico—are all long odds. For the most part, trends in security are moving in positive directions for U.S. interests. Democratic institutions, the expansion of free markets, peaceful settlement of disputes, and promotion of collective security are diminishing state-to-state threats to U.S. interests.[50]

Russia and China, the two most likely peer-competitors on the 15-year horizon, seem to have governments with which the United States can work on common interests and manage areas of divergence. North Korea, Iran, and Iraq—the usual suspects for state-to-state threats when Russia and China are excluded—all appear to be moving in directions conducive to U.S. interests. For the most part, America is in clover as far as threats to our interests from other states are concerned.

However, as this paper has attempted to demonstrate, the United States should not become complacent about its current good fortune. As we have seen, several types of state-to-state threats could develop that would dramatically impair the U.S. ability to carry out its current security policies.

Some of these situations the United States is unable to control or even materially affect. However, most of them are

amenable to U.S. pressure and influence, provided that careful attention is paid to early detection and management. Sensible diplomacy, targeted aid, help to allies in resolving domestic problems, and the selective use of military force can defuse or ameliorate many of these potential problems.

General John Galvin, the former Supreme Allied Commander Europe, has remarked that if someone had told him when he became SACEUR in 1986 that NATO's first combat operations would be as part of a 35-nation coalition fighting to repel an Iraqi invasion of Kuwait, he would not have believed it. This insight illustrates the inescapable uncertainty of the international environment, especially now that Cold War inhibitions on the use of force have been dissolved. While none of the specific state-to-state threats identified in this paper may be probable, they, and others like them, are perhaps no less likely than the challenge posed in 1991 by Iraq and the American-led response to that threat.

ENDNOTES

1. International Institute for Strategic Studies, *The Military Balance, 1997/98*, London: Oxford University Press, 1997, p. 165.

2. Sang Hoon Park, "North Korea and the Challenge to the US-South Korean Alliance," *Survival*, Vol. 36, No. 2, Summer 1994, p. 87.

3. International Institute for Strategic Studies, *Strategic Survey 1996/97*, London: Oxford University Press, 1997, p. 183.

4. Marcus Noland, "Why North Korea Will Muddle Through," *Foreign Affairs*, Vol. 76, No. 4, July/August 1997, p. 117.

5. "A President Spooked," *The Economist,* April 11, 1998, p. 30.

6. "Koreas Agree to Talks," *The Washington Post*, April 7, 1998, p. A17.

7. "N. Korea Urged to Clarify Offer on Talks," *The Washington Post*, March 19, 1998, p. A30.

8. Denny Roy, "North Korea as an Alienated State," *Survival*, Vol. 38, No. 4, Winter 1996-97, p. 27.

9. Nicholas Eberstadt, "Hastening Korean Reunification," *Foreign Affairs*, Vol. 76, No. 2, March/April 1997, p. 79.

10. Christopher W. Hughes, "The North Korean Nuclear Crisis and Japanese Security," *Survival*, Vol. 38, No. 2, Summer 1996, p. 95.

11. Nicholas Eberstadt, pp. 84-85.

12. Anthony Lake, "Confronting Backlash States," *Foreign Affairs*, Vol. 73, No. 2, March/April 1995, p. 52.

13. Zalmay Khalilzad, "The United States and the Persian Gulf: Preventing Regional Hegemony," *Survival*, Vol. 37, No. 2, Summer 1995.

14. International Institute for Strategic Studies, *The Military Balance 1997/98,* p. 116.

15. Shahram Chubin and Charles Tripp, *Iran-Saudi Arabia Relations and Regional Order*, Adelphi Paper 304, London: Oxford University Press, 1996, p. 4.

16. Fawaz Gerges, "Washington's Misguided Iran Policy," *Survival*, Vol. 38, No. 4, Winter 1996-1997, p. 6.

17. Shahram Chubin, "Does Iran Want Nuclear Weapons?" *Survival*, Vol. 37, No. 1, Spring 1995, p. 88.

18. Thomas W. Lippman, "More Signs of Thaw in Icy U.S.-Iran Relations," *The Washington Post*, p. A28.

19. Ahmed Hashim, *The Crisis of the Iranian State*, Adelphi Paper 296, London: Oxford University Press, 1995, p. 3.

20. "Never the Twain Shall Meet," *The Economist*, April 11, 1998, p. 33.

21. "Helping Khatemi," *The Economist,* April 11, 1998, p. 13.

22. The Clinton Administration rejected the deal under the more stringent embargo guidelines adopted in 1995. The contract was subsequently awarded to the French Total consortium, triggering possible U.S. sanctions against France under the Iran-Libya Sanctions Act.

23. For excellent critiques of dual containment, see F. Gregory Gause III, "The Illogic of Dual Containment," *Foreign Affairs*, Vol. 73, No. 2, March/April 1995; Zbigniew Brzezinski, Brent Scowcroft, and Richard Murphy, "Differentiated Containment," *Foreign Affairs*, Vol. 76, No. 3, May/June 1997; and Fawaz Gerges.

24. Jahangir Amuzegar, "Adjusting to Sanctions," *Foreign Affairs*, Vol. 76, No. 3, May/June 1997, p. 31.

25. Ofra Bengio, "The Challenge to the Territorial Integrity of Iraq," *Survival*, Vol. 37, No. 2, Summer 1995, p. 85.

26. Aziz Abu-Hamad, "Gulf State No-Shows," *The Washington Post*, 20 March 1998, p. A23; see also Richard Engel, "Saudis Move Closer to Iran," *Washington Times*, April 6, 1998, p. 1.

27. Gause, p. 62.

28. Countering this prospect is the recent warming in relations between Saudi Arabia and Iran. See Robert S. Greenberger and Thomas E. Ricks, "Iran's Diplomatic Moves Puzzle the U.S.," *Wall Street Journal*, March 19, 1998, p. 14.

29. Graham E. Fuller and Ian O. Lesser, "Persian Gulf Myths," *Foreign Affairs*, Vol. 76, No. 3, May/June 1997, p. 50.

30. South Korea and its *chaebol* model of state-sponsored capitalism are also experiencing a severe economic crisis. The security situation of South Korea, and its long-standing close association with the United States make it an unlikely participant in any anti-U.S. coalition.

31. Adam Schwarz, "Indonesia After Suharto," *Foreign Affairs*, Vol. 76, No. 4, July/August 1997, p. 125.

32. Ofra Bengio, pp. 82-84.

33. "Kosovo Albanians Charged as Officials Tour Balkans," *The New York Times*, 18 March 1998.

34. For a useful model of the dynamic of intergroup conflict, see Roderick von Lipsey, ed., *Breaking the Cycle: A Framework for Conflict Intervention*, New York: St. Martin's Press, 1997.

35. Philip G. Smucker, "The Road to a New Balkan Hell," *U.S. News and World Report*, April 13, 1998, p. 36.

36. The seriousness of a Kosovo contingency prompted President Bush in 1991 to threaten action against Serbia if an outbreak of violence occurred there; the threat was repeated by President Clinton.

37. "The Kosovo Cauldron," *The Economist*, March 14, 1998, p. 53.

38. "UN Official Fears Flood of Kosovo Refugees," *The Washington Post*, March 29, 1998, p. A23.

39. "Mesmut Yilmaz, Ambivalent Turk," *The Economist*, March 14, 1998, p. 60.

40. Fouad Ajami, "The Sorrows of Egypt," *Foreign Affairs*, Vol. 74, No. 5, September/October 1995, p. 88.

41. *Ibid*., pp. 85-86.

42. Graham E. Fuller and Ian O. Lesser, pp. 46-47.

43. "When Gulf States Tighten Their Belts," *The Economist*, March 14, 1998, p. 49.

44. "Oil Prices Hit Lowest Level in Ten Years," *The Washington Post*, March 18, 1998, p. 1.

45. Tim Golden, "Mexican Military Helps Drug Traffickers, U.S. Reports Say," *The New York Times*, March 26, 1998, p. 1.

46. Dana Priest, "U.S. May Boost Military Aid to Colombia's Anti-Drug Effort," *The Washington post*, March 28, 1998, p. A19.

47. "Mexico admits drug traffickers bought bank," *Financial Times*, March 17, 1998, p. 1.

48. Molly Moore, "Corrupt From the Top: Drug-Running by High Officials Jars Mexican State," *The Washington Post*, March 29, 1998, p. A22.

49. "Colombia Creates Anti-Guerrilla Force," *The Washington Post*, March 13, 1998, p. A18.

50. Anthony Lake, p. 45.

PART IV: ROUNDTABLE ON FUTURE RESPONSES—

John Allen Williams
Timothy A. Kinnan
Robert H. Scales, Jr.

Summary.

Panel Chairman Dr. John Hillen opened discussion with an admonition against the tendency of many American defense thinkers to connect U.S. vulnerabilities directly with strategies, capabilities, and intentions of shadowy, unidentified "enemies." No nation, not even the United States, can eliminate all its vulnerabilities. Rather, we as a nation must narrow our security focus to those particular vulnerabilities that correlate with actual capabilities and intentions on the part of real-world enemies. With regard to defense thinkers in general, he makes the additional point that the United States has precious few defense thinkers—perhaps a dozen—who see deeply into the human condition as the wellspring of war and conflict. We must contrive to produce many more such thinkers who instinctively divine that we can never understand the nature of the threat to our security and survival unless we understand the nature of Homo sapiens himself.

Dr. John Allen Williams adduced four overarching themes. First was the utility of history in preparing for the future. The problem is not that we ignore history. The problem, rather, is that we do hearken to history but misapply its lessons, e.g., in applying the lesson against appeasement learned from Munich in 1938 to the situation in Vietnam in 1965. His second theme was the difficulty in dealing with complexity and nonlinearity. Defining the true national interest, for instance, is complicated by the participants' tacit political, career, and economic interests, which figure in deliberations but have nothing intrinsically to do with national interests. Systems analysis, ever

mechanistic, still reigns, though it has little utility in attacking the often decisive human dimension of strategic problems.

Dr. Williams' third theme was the role of reserve forces. There is plenty of work to go around in an age of declining defense budgets and thus no need for the present fiscal food fights. The reserves pull their weight, not only with their special capabilities but also as a valuable link between the military and civil society. The fourth theme was the poor U.S. record in dealing with ambiguous conflicts. Give us back the Cold War and a conventional opponent, and U.S. forces would be well nigh invincible. But give us unconventional war or terrorism, and suddenly the outcome is dicey.

Going beyond the foregoing themes, Dr. Williams makes a plea for greater flexibility in military planning directed to the distant future; for greater appreciation of asymmetrical advantages the United States can apply against enemy disadvantages; for consideration of broader participation by the professional military in the nation's defense dialogue; for increased attention to problems posed by the cultural gap between the military and civilian society; and for rewarding people who think constructively out of the box of prevailing orthodoxy.

Major General Timothy A. Kinnan elaborated upon a single theme: the present absence of a true dialogue among the uniformed services concerning strategy and warfighting. What usually masquerades as dialogue is sly digs at the other services' agendas rather than objectively presented solutions to the problems at hand. For example, rather than simply explaining the efficiency and effectiveness of aerial technology in halting an advancing enemy, the airman instead accuses the soldier of indifference to casualties in proposing a force-on-force response. Or, faced with disagreement from the airman on the issue, the soldier rejoins that the airman doesn't

understand war because he never smells cordite in the foxhole and never holds a dying buddy in his arms.

Any *ad hominem* thrust of this nature—whether it impugns the other side's motives or its insight—instantly halts dialogue and renders agreement impossible. Anger, insult, and sarcasm have replaced objective analysis in interservice discourse because of one underlying reality: the struggle for resources in a fiscally constrained environment. Each service believes it can protect its resources by achieving a more prominent role in future military operations and war plans. Hence most interservice discussion of tactics, operations, and strategy today is in fact a thinly disguised struggle for resources. It should be the aim of all participants to banish preoccupation with resources from their minds and to focus instead upon the optimum military solution. Disagreements may still occur, but at least those disagreements will occur within the context of genuine debate.

As budgets fall faster than force structure, it is tempting to throw out expensive technology as a means of preserving force structure. But rather than concerning ourselves so single-mindedly with force structure, we need to concentrate instead upon how best to accomplish the assigned missions with whatever force structure remains. Technology can help us do that. Technology, by providing a real-time picture of the battle space plus command and control mechanisms for integrating the battle systems of all service components in a seamless web of coordinated action, enables us to quit drawing lines to govern where we fight. No longer would we have to sunder battle space, assigning sacred parcels of turf to each of the components, with all the loss of efficiency and synergy that such a fractionated system entails. Instead, we would impose a genuinely joint effort throughout every cubic inch of the theater battle space, thus achieving maximum efficiency from the total force available.

If the services start thinking of themselves as partners rather than adversaries, the budget allocation process will proceed far more smoothly, and we can save our bullets for the enemy.

During the question-and-answer period, replying to a questioner who attributed present service disunity to the Quadrennial Defense Review (QDR), General Kinnan replied that the QDR is a symptom, not a cause. Interservice friction results from insufficient budget to accomplish the tasks assigned. The services must find the strength to rise above this shortfall.

Major General Robert H. Scales, Jr., framed his remarks as a series of impressions. During a lengthy trip prior to taking up his present billet, he visited the militaries of 13 countries around the world, including those of Russia and China. He encountered four recurring questions:

(1) How do you build an NCO corps?

(2) How do you integrate women into a military force?

(3) How do you professionalize the military of an emerging state, keeping it subordinate to civilian authority?

(4) How did the United States and its allies accomplish their striking victory in the Gulf War of 1991?

The younger officers are highly professional; they are bent not upon borrowing U.S. technology, but rather its ethos, culture, and methods. American field manuals are ubiquitous; American military materials are harvested from the Internet; China is one of the largest consumers of U.S. military literature.

With regard to *Joint Vision 2010*, the Joint Chiefs of Staff (JCS) Chairman's vision of future war, an unintended consequence of it apparently is the gradual division of the offensive function into *precision engagement*, to be performed by the Navy and Air Force, and *dominant maneuver*, to be performed by the Army and Marines.

Instead of a convergence of these two elements as witnessed in the Gulf War, General Scales sees divergence, which to him is troubling.

As to the relative priority of precision engagement and dominant maneuver, neither should receive priority over the other. Rather we should seek a balance between the two. It is impossible at this remove to be certain of the nature of the threat prevailing beyond the critical year of 2010. To hedge our bets, we must build toward ample capability both in reaching out to strike the enemy and in out-maneuvering him when we close. Though our goal is indeed to mold a true joint force, we must do so without dissolving service identities. Soldiers, sailors, marines, and airmen fight out of pride in what they are; we must not tinker with this vital factor in *esprit* and combat motivation.

Returning to the theme of uncertainty, General Scales emphasizes that, in planning the force that will take the field in the years beyond 2010, we must prepare to operate anywhere along the spectrum of conflict, ranging from purely service operations like hurricane relief on one end to ultimate combat such as theater nuclear war on the other. To prophesy at this time the precise points on the spectrum of conflict where we'll be operating 15 years from now, and then to build a force based on that prophecy, are to invite disaster.

In capitalizing upon the technology associated with the Information Age, General Scales counsels against rushing in too quickly, trying to assimilate the new tools in one gulp. Like the Iron Age and the Industrial Age before it, the Information Age will unfold through time, consolidating and defining itself as it evolves. The same is true for Information Age warfare, which no one can suddenly invent, but which rather must develop organically at its own pace over the coming decades, taking turns and assuming forms that are undiscernible to us today. Our best posture is vigilant observation, active trial-and-error, and continued adaptation, keeping our eye always on the longer-range

picture. We should give up our neurotic insistence on inventing Information Warfare at a single bound. Rather than attempting to accelerate the technology artificially with huge investments of military research money, our best bet is to borrow wisely from the commercial sector, which is already churning out products and applications faster than we can conceive them. By taking a more measured approach to preparing for future war, we lessen chances of compounding our errors, wasting our resources, and getting our people killed unnecessarily.

In thinking about future war, rather than technology we should be concerned primarily with these four areas: leader development, training and education, doctrine, and experimentation. All are challenging because they require long lead times, with leader development taking the longest time, more so even than technology. It takes 17 years to develop a battalion commander, 17 for a platoon sergeant.

A vision of future warfare is, of course, necessary, but the vision is never static, fixed for all time, but rather is dynamic, refining itself constantly by an iterative process to take account of new developments. From the maturing vision, we draw concepts. From the concepts, we design forces and doctrine. We are headed in the right direction. For the next 10 years or so, we have the luxury of a period of calm deliberation. There is no hurry. We have the time and opportunity to do it right. Let's not become so busy in our obsession with effecting change that, despite our intelligence, we act stupidly. Brilliance in operational technique is a good thing, but an intellectual grasp of the larger patterns of war and history is essential, too, if we are to avoid the mistakes of past generals who failed to master the discontinuities of time and fortune.

During the question-and-answer period, a questioner wondered whether, in the coming age of domestic terrorism, we shouldn't get rid of the *posse comitatus* law, which forbids the use of U.S. armed forces to enforce civil laws. General Scales stated that the authors of the law knew what

they were doing, and that for a host of reasons it is best not to involve the Federal Armed Forces directly in civil law enforcement. In response to a question regarding the present lack of a military peer competitor for the United States, General Scales observed that if we continue unilaterally reducing our present conventional military dominance, we might thereby create peer or major competitors.

BIOGRAPHICAL SKETCHES

Major General Edward B. Atkeson, U.S. Army, Retired, is a Senior Fellow of the Institute of Land Warfare, AUSA, and a private consultant on national and international security affairs. His final assignment prior to retirement from the Army in 1984 was to the National Intelligence Council where he served as National Intelligence Officer for General Purpose Forces. He also served with the Bureau of Political/Military Affairs, Department of State; as a Fellow at the Center for International Affairs, Harvard University; and on the faculty of the U.S. Army War College. He has contributed over 50 articles to various publications and has authored one book, *The Final Argument of Kings: Reflections on the Art of War.* In the present conference, General Atkeson chaired Panel III–Threats

Dr. Stephen J. Blank is Associate Professor of Russian/Soviet Affairs at the Strategic Studies Institute. He is the editor of *Imperial Decline: Russia's Changing Position in Asia*, coeditor of *Soviet Military and the Future*, and author of *The Sorcerer as Apprentice: Stalin's Commissariat of Nationalities, 1917-1924.* He has also written many articles and conference papers on Russian, CIS, and Eastern European security issues. Dr. Blank's current research deals with proliferation and the revolution in military affairs, and energy and security in Eurasia. He holds a B.A. in History from the University of Pennsylvania, and an M.A. and Ph.D. in History from the University of Chicago.

Dr. Robert J. Bunker attended California State Polytechnic University, Pomona, and the Claremont Graduate University where he earned an M.A. in Government and a Ph.D. in Political Science. He is an Adjunct Professor in the National Security Studies Program at California State University, San Bernardino, and is the Professor of Unconventional Warfare at American Military

University of Manassas, Virginia. His articles have appeared in numerous publications including *Parameters, Special Warfare, Military Intelligence*, and the *Airpower Journal*. Dr. Bunker's conference presentation, "Five-Dimensional (Cyber) Warfighting: Can the Army After Next Be Defeated through Complex Concepts and Technologies?", is not included in the present volume as it has been published separately by the Strategic Studies Institute.

Dr. Donald D. Chipman is on the faculty of Air University. He is an advisor to the Commandant of Squadron Officer School and teaches a course on strategic thought. Dr. Chipman attended Florida State University where he earned a Master's and Ph.D. in Educational History and Philosophy. He has coauthored two books: *Philosophical Reflections on Education* and *Critical Issues in Philosophy of Education,* and his articles have appeared in *Military Review, Armed Forces International*, *Marine Corps Gazette* and *Airpower Journal.* He served 26 years of reserve and active duty, retiring from the Navy in 1989. In the present conference, Dr. Chipman chaired Panel IV–State-on-State Approaches.

Colonel Robert A. Doughty is the Head of the Department of History at the U.S. Military Academy. He graduated from the Academy in 1965 and received his Ph.D. in European History from the University of Kansas. He is a graduate of the Command and General Staff College. His most recent book is *Warfare in the Western World, Volumes I and II*. He has also published *The Breaking Point: Sedan and the Fall of France, 1940*. He is currently working on a book manuscript tentatively titled *Pyrrhic Victory: French Military Strategy and Operations During the Great War.*

Colonel Charles J. Dunlap, Jr., is the senior legal counsel for U.S. Strategic Command. A graduate of St. Joseph's University and Villanova University School of Law, he is also a Distinguished Graduate of National War College. Colonel Dunlap has served in a variety of military

assignments in the United States, Europe, Asia, Africa, and the Middle East. A noted speaker and writer on national security issues, his articles include "The Origins of the American Military Coup of 2012"; "How We Lost the High Tech War of 2007"; and "Sometimes the Dragon Wins: A Perspective on Information Age Warfare."

Mr. Edmund M. Glabus is the Director of Advanced Concepts and Technologies Group, Aegis Research Corporation. A graduate of the Georgetown University School of Foreign Service, he has conducted graduate work at the Joint Military Intelligence College, Defense Intelligence Agency, and American Military University. He is a professional member of the World Future Society. Mr. Glabus has held a variety of Army command and staff positions in the United States and overseas. He is the creator of InfoChess™, a competitive strategy learning game used by several DoD agencies.

Dr. John F. Guilmartin, Jr., is an Associate Professor of History at The Ohio State University. He received his B.S. in Aerospace Engineering from the USAF Academy and his M.A. and Ph.D. in History from Princeton University. He is well known among naval historians for his book, *Gunpowder and Galleys: Changing Technology and Mediterranean Warfare at Sea in the Sixteenth Century.* Dr. Guilmartin is the primary author of *Encyclopedia Britannica's* article on the technology of war. His most recent book is *A Very Short War: The Mayaguez and the Battle of Koh Tang*, an account of America's last battle of the Vietnam War.

Dr. John Hillen is the Olin Fellow for National Security Studies at the Council on Foreign Relations. A former Army officer, he served in Europe, the Pacific, and Southwest Asia. He graduated with a Fulbright Scholarship from Duke University, and earned his Master's degree in War Studies at King's College London, and his doctorate in International Relations from Oxford University. He has published articles on international security issues in *Foreign Affairs, Orbis,*

The International Herald Tribune, The Wall Street Journal, and other journals. He is the author of *Blue Helmets: The Strategy of UN Military Operations*. In the present conference, Dr. Hillen chaired Panel V–Roundtable on Future Responses.

Major General Timothy A. Kinnan is Commandant, Air War College, and Vice Commander, Air University. During his career, he has been assigned to numerous operational, command, and staff positions, including four tours in NATO, and he has commanded a fighter squadron and two wings. Prior to assuming his current position, he served as Deputy Commander of Headquarters 5th Allied Tactical Air Force (NATO), Vicenza, Italy. General Kinnan holds a Bachelor's degree in Astronautical and Aeronautical Engineering from the U.S. Air Force Academy and a Master's in Astronautical and Aeronautical Engineering from Purdue University.

Colonel James H. Kurtz, U.S. Army, Retired, served over 30 years in the U.S. Army where he held a variety of troop leading, command and staff assignments. He was Chief of Staff of the President's Commission on Critical Infrastructure Protection, which examined the interconnections of the nation's infrastructures, explored their vulnerabilities to emerging threats, both physical and cyber, and recommended a comprehensive national policy for protecting these infrastructures and assuring their continued operation. He holds a B.S. from Cameron University and an M.A. from Webster University, and is a graduate of the U.S. Army Command and General Staff College and the National War College. In the present conference, Colonel Kurtz chaired Panel II–Threats.

Colonel Lloyd J. Matthews, U.S. Army, Retired, graduated from the U.S. Military Academy, he has a M.A. from Harvard University and a Ph.D. from the University of Virginia, and is a graduate of the Armed Forces Staff College and the Army War College. Overseas tours included Germany and Vietnam. In other assignments, he was a

battalion commander; editor of *Parameters,* the U.S. Army War College Quarterly; and Associate Dean of the U.S. Military Academy. He is the editor of five books *Assessing the Vietnam War* (1987), *The Parameters of War* (1987), *The Challenge of Military Leadership* (1989), *The Parameters of Military Ethics (1989),* and *Newsmen and National Defense* (1991), the first four having been co-edited with Dale Brown. Additionally, he is the author of some 60 articles, features, and reviews on military topics, in such journals as *Parameter*s, *ARMY Magazine, Military Review*, and *Airpower Journal*.

Dr. Steven Metz is an Associate Research Professor in the Strategic Studies Institute and holds the Henry L. Stimson Chair in Military Studies at the Army War College. He joined SSI in 1993 after serving as an Associate Professor of Low Intensity Conflict and Third World Studies at the Air War College. He has written extensively on a variety of national and international security topics and has testified before the Africa subcommittees of the U.S. Senate and House of Representatives. Dr. Metz earned his B.A. in Philosophy and M.A. in International Studies from the University of South Carolina and his Ph.D. in Political Science from Johns Hopkins University.

Dr. Donald J. Mrozek is Professor and Chair of the Department of History at Kansas State University. He took his A.B. degree at Georgetown University and his M.A. and Ph.D. at Rutgers University. He has written two books including *Air Power and the Ground War in Vietnam*, and is coeditor of the series *A Guide to the Sources of United States Military History.* Dr. Mrozek has published articles in U.S. journals such as *Military Affairs* and *Business History Review* and in overseas journals such as *Military History* (Beijing) and *Military Historical Research*. He is currently revising a book manuscript on how the U.S. armed forces interpreted the Vietnam War in the late 1970s and 1980s.

Dr. Stephen C. Pelletiere has served as SSI's Middle East expert since 1988 and is a Research Professor of National

Security Affairs. Prior to this appointment, he was an intelligence officer in Washington monitoring the Iran-Iraq War. Dr. Pelletiere is the author of *The Iran-Iraq War: Chaos in a Vacuum* and other books and monographs. He earned his B.A. in English from the University of Vermont and his Ph.D. in Political Science from the University of California, Berkeley. His latest SSI publication is *The Peace Process, Phase I: Past Accomplishments and Future Concerns.*

Lieutenant Colonel Ralph Peters, U.S. Army, Retired, recently retired from the U.S. Army after two decades of service. His assignments in the Army were located in many areas of the world and were focused mainly in the intelligence field. A prolific writer, his articles principally have concerned strategy, military theory, and ethics. He also has written seven novels, the most recent being *The Devil's Garden*, which concerns oil and diplomacy in Azerbaijan. Colonel Peters lectures on strategic and cultural issues and contributes to various newspapers and journals.

Dr. Jeffrey Record is a Visiting Professor at the Air War College from Georgia Tech's Sam Nunn School of International Affairs. He is also a Senior Research Fellow at Tech's Center for International Strategy, Technology and Policy. Dr. Record is the author of numerous books and monographs, including *Hollow Victory: A Contrary View of the Gulf War; Revising U.S. Military Strategy: Tailoring Means to Ends;* and *The Wrong War: Why We Lost in Vietnam* (forthcoming). He received a B.A. in Political Science from Occidental College, and an M.A. and Ph.D. in International Politics from the Johns Hopkins School of Advanced International Studies. Dr. Record's conference presentation, "The Creeping Irrelevance of U.S. Force Planning," is not included in the present volume as it has been published separately by the Strategic Studies Institute.

Major General Robert H. Scales, Jr., has been Commandant of the U.S. Army War College since August 1997. He graduated from the United States Military Academy and subsequently earned a Master's and Ph.D. in History from Duke University. He is also a graduate of the Armed Forces Staff College and the Industrial College of the Armed Forces. He is principal author of *Certain Victory*, the official Army account of the Gulf War. *Firepower in Limited War*, a history of fire support in post-World War II conflicts, is his latest work. Prior to his present assignment, General Scales was Deputy Chief of Staff for Base Operations and then Deputy Chief of Staff for Doctrine at Headquarters, U. S. Army Training and Doctrine Command.

Dr. Kori N. Schake is a Postdoctoral Scholar at the Institute on Global Conflict and Cooperation at the University of California at San Diego. She holds a Ph.D. in Political Science from the University of Maryland and has previously worked for the Assistant Secretary of Defense for Strategy and Requirements and as the NATO Desk Officer in the Directorate for Strategic Plans and Policy in the Joint Staff.

Dr. Stephen Sloan is a Professor of Political Science at the University of Oklahoma. He received his Ph.D. and M.A. degrees in Comparative Politics from the Graduate School of Arts and Sciences at New York University, and his B.A. from Washington Square College of New York University. Dr. Sloan's latest books are: *Low-Intensity Conflict: Old Threats in a New World*, coedited with Edwin G. Corr; *Corporate Aviation: The Next Frontier in Aerospace Operations*, coauthored with Harry Pier; and *Historical Dictionary of Terrorism*, coauthored with Sean Kendal Anderson. He also was an expert contributor to the Vice President's Task Force on Combating Terrorism.

Mr. Robert D. Steele is a retired Marine Corps infantry and intelligence officer. He is the founder and president of Open Source Solutions, Inc. and is an expert on computer

and information vulnerabilities. Mr. Steele holds on A.B. in Political Science from Muhlenberg College and Master's degrees in International Relations from Lehigh University and Public Administration from the University of Oklahoma. He has also earned certificates in intelligence policy from Harvard University and in defense studies from the Naval War College.

Dr. Earl H. Tilford, Jr., has been Director of Research at SSI since 1993. He retired from the U.S. Air Force in 1989. In his career he served as an intelligence officer, instructor at the Air Force Academy, and editor of *Air University Review*. Dr. Tilford is the author of three books, the latest being *Crosswinds: The Air Force's Setup in Vietnam*. He also coedited *Eagle in the Desert: A Look Back at the U.S. Military in the Persian Gulf*. He has authored numerous articles and conference papers. Dr. Tilford earned his B.A. and M.A. in History from the University of Alabama and his Ph.D. in History from George Washington University. In the present conference, Dr. Tilford chaired Panel I–Symmetries and Asymmetries–A Historical Perspective.

Dr. John Allen ("Jay") Williams is Associate Professor, Department of Political Science, Loyola University of Chicago. He received his B.A. from Grinnell College, and his M.A. and Ph.D. from the University of Pennsylvania. He coauthored *Soldiers, Society, and National Security*, and coedited and contributed to *The U.S. Army in a New Security Era*. He is currently coediting a book, *The Postmodern Military: Armed Forces After the Cold War*. He has published in *Armed Forces and Society, The Washington Quarterly, Military Review, America, Air University Review*, and the Naval Institute *Proceedings*.