REPORT DOCUMENTATION PAGE

. **Report Security Classification**: UNCLASSIFIED

. **Security Classification Authority**:

. **Declassification/Downgrading Schedule**:

. **Distribution/Availability of Report**: DISTRIBUTION STATEMENT A: APPROVED FOR UBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

. **Name of Performing Organization**:
JOINT MILITARY OPERATIONS DEPARTMENT

. **Office Symbol**:	**7. Address**: NAVAL WAR COLLEGE
C	686 CUSHING ROAD NEWPORT, RI 02841-1207

. **Title** (Include Security Classification): OPERATING BEYOND THE "BOX": WINNING IN THE ASYMMETRIC ATTLESPACE (UNCLASSIFIED)

. **Personal Authors**: Major Ossen J. DHaiti, USMC

0.**Type of Report**: FINAL	**11. Date of Report**: 03 FEBRUARY 2003

2.**Page Count**: 30 **Paper Advisor: Professor Davis Goodrich**

3.**Supplementary Notation:** A paper submitted to the Faculty of the NWC in partial atisfaction of the requirements of the JMO Department. The contents of this paper eflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

4. **Ten key words that relate to your paper:**

symmetric Warfare, Unrestricted Warfare, Mindset, Operational Strategy, Operational Capability, Asymmetric Maneuver Space, COCOM Staff, Black ell, Threat Response, Civil-Military

5.**Abstract:** Today's American way of war, born out of the mostly bi-polar Cold War environment, demonstrates a mindset derived from US cultural, tellectual, and political history that has shaped it to the conclusion that there is one ideal way of making war and making peace. This paradigm has een supplanted by an asymmetric threat paradigm characterized by radically unconventional, non-linear, and unconstrained strategies perpetrated by dversaries of mostly non-governmental and non-state actors designed to exploit critical US vulnerabilities. The synchronized and coordinated terrorist tack on September 11th, 2001 can be considered the watershed event compelling unprecedented reformation of the US National Security system ffecting every instrument of national power. Focusing specifically at the military instrument of power, it is the contention of this author that current perational capability can only yield limited success for it lacks the appropriate "tools and skill sets" vis-à-vis the adversary applying asymmetric rategies. Bounded at the operational level, this analysis proposes a fundamental change in mindset, emphasis on the right "tools," and a strategy rooted asymmetric warfare itself. A resultant by-product of this analysis is the establishment of a "Black Cell" within the COCOM staff whose function is to rmulate asymmetric strategies to place the Operational Commander in a better position to win in the asymmetric battlespace.

6.**Distribution / vailability of bstract:**	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

7.**Abstract Security Classification**: UNCLASSIFIED

8.**Name of Responsible Individual**: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

9.**Telephone:** 841-6461	**20.Office Symbol: C**

Security Classification of This Page Unclassified

NAVAL WAR COLLEGE
Newport, R.I.

OPERATING BEYOND THE "BOX": WINNING IN THE ASYMMETRIC BATTLESPACE

By

Ossen J. DHaiti
Major, United States Marine Corps

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

03 February 2003

_____

Prof. David Goodrich
Professor, JMO Department

Abstract of

OPERATING BEYOND THE "BOX":
WINNING IN THE ASYMMETRIC BATTLESPACE

Today's American way of war, born out of the mostly bi-polar Cold War environment, demonstrates a mindset derived from U.S. cultural, intellectual, and political history that has shaped it to the conclusion that there is one ideal way of making war and making peace. This paradigm has been supplanted by an asymmetric threat paradigm characterized by radically unconventional, non-linear, and unconstrained strategies perpetrated by adversaries of mostly non-governmental and non-state actors designed to exploit critical U.S. vulnerabilities. The synchronized and coordinated terrorist attack on September 11, 2001 can be considered the watershed event compelling unprecedented reformation of the U.S. National Security system affecting every instrument of national power. Focusing specifically on the military instrument of power, it is the contention of this author that current U.S. military operational capability can only yield limited success for it lacks the appropriate "tools and skill sets" vis-à-vis an adversary applying asymmetric strategies. Bounded at the operational level, this analysis proposes a fundamental change in mindset, emphasis on the right "tools," and a strategy rooted in asymmetric warfare itself. A resultant by-product of this analysis is the establishment of a "Black Cell" within the COCOM staff whose function is to formulate asymmetric strategies to place the operational commander in a better position to win in the asymmetric battlespace.

TABLE OF CONTENTS

PREFACE

If perception is reality, then the reality is this: today, the United States military stands alone as the hyper-power and the basis upon which American global dominance is built. This outcome was not accidental, but a deliberate effort during the better part of the 20th century to deter any potential military foe. Having defeated its closest rival, which ended the Cold War, the U.S. military is the epitome of strength and dominance. Directly challenging such a force on the battlefield today is a futile undertaking, as the 1990-1991 Gulf War magnificently proved.

As did the British during the age of British imperial dominance and Pax Britannica (British Peace), the United States stands as leader of the world. This, however, does not mean that United States power is uncontested or even welcomed; in fact, the contrary is more likely. All things equal, the 21st century will be the age of "Pax Americana." Because of the outright dominance of U.S. military might, potential adversaries of the United States—state and especially non-state—who reject the notion of Pax Americana have been driven to seek other "means" to level the playing field. Most potential adversaries in the foreseeable future see that the only means of succeeding against the United States are those rooted firmly in asymmetric strategies.

The nature of the threat today—and increasingly more so tomorrow—is of emerging alliances of state and non-state adversaries exploiting asymmetric strategies designed to attack critical U.S. military and non-military vulnerabilities across the spectrum of conflict. The synchronized and coordinated terrorist attacks on September 11, 2001 can be considered the watershed event compelling unprecedented reformation of the U.S. national security

system, affecting every instrument of national power. Focusing specifically at the military instrument of power, it is the goal of this analysis to point to the inadequacy of current measures against asymmetric strategies and to explore other possible measures.

I
INTRO

Like War itself, our approach to warfighting must evolve. If we cease to refine, expand, and improve our profession, we risk becoming outdated, stagnant, and defeated.

General A.M. Gray, USMC, MCDP-1 Warfighting

At a Capitol Hill Hearing before the House Armed Services Committee on 27 February 2002, General Tommy R. Franks, Commander, U.S. Central Command (USCENTCOM), testified that:

> Our adversaries will pursue asymmetric capabilities and strategies. Their attacks will focus on U.S. national will, coalition unity, and world opinion. Adversaries will attempt to inflict U.S. casualties, defeat our precision strike capabilities, deny access, and prevent us from achieving information and battlespace superiority.[1]

As will be discussed in this paper, the Commander of USCENTCOM has used the word ***asymmetric*** not in the usual context of the traditional threat paradigm, but in a newer, more complex context to denote a departure from the very notion of the Western contrived conventional threat paradigm. A conventional threat paradigm demonstrative of a mindset derived from U.S. cultural, intellectual, and political history that has shaped it to the conclusion that there is one ideal form of government, which suggests one ideal way of making war and making peace.[2] Today's American way of war is characterized by the conduct of large-scale, sustained combat operations where the goal is to win quickly and decisively with as few casualties as possible. This conventional threat paradigm that emphasizes conventional forces, nuclear deterrence, well-understood rules of engagement and doctrine, the rule of law, and easy-to-detect intelligence indicators has been supplanted by a bolder, more complex asymmetric threat paradigm.

Today, the asymmetric threat paradigm is defined by radically unconventional, random, non-linear, anarchistic, disproportionate, and unconstrained strategies perpetrated by mostly

non-governmental and non-state actors. While the few definitions of asymmetric warfare associate it with a strategy used by a weaker adversary or by an adversary seeking to avoid enemy strengths, the definition proposed in this analysis will not limit it as such. This author defines asymmetric warfare as the employment of innovative measures beyond restrictions and boundaries on *all* factors relating to one's adversary, dispersed in time and space within and beyond the military sphere, where military and non-military capabilities are of equal footing in the accomplishment of the objective during the entire course of conflict. This definition does not make mention of any weapon systems or their use in some "different" manner, as would the old paradigm meaning of asymmetry; rather it is rooted in a mindset—a way of thinking. Like most innovations in warfare, asymmetry as defined above has been born out of necessity.

The pursuit of asymmetric capabilities and strategies outlined by General Franks before the House Armed Services Committee is a viable alternative for state and non-state actors. Today's Combatant Command (COCOM) must orient its capabilities with respect to the asymmetric threat paradigm and—to use a strike pilot adage—"honor the nose [weaponry] of the threat." That is, if a change in course is required to re-orient capabilities to maintain an advantageous position—or at worst, keep from getting into a disadvantageous position—then that action must be taken in light of the threat. At the heart of that re-orientation must be the realization that these are enemies whose visions, objectives, means, and theories of victory (TOV) are acutely different from United States' own technologically-based preconceptions. The current mindset of the vast majority of U.S. military professionals and organizations may leave them vulnerable to asymmetric challenges that arise from adversaries of a very different cultural and geo-political perspective. How does the U.S.

military, specifically at the theater commander or Joint Task Force level, fight and win in an asymmetric warfare arena? Based on sound understanding of the nature of the asymmetric threat, the operational commander can fight and win against such a threat, only if there is a fundamental change in mindset, emphasis on other "instruments," and a strategy rooted in asymmetric warfare itself.

II
MINDSET

If in the days to come mankind has no choice but to engage in war, it can no longer be carried out in the ways with which we are familiar...what we are referring to are not changes in the instruments of war, the technology of war, the modes of war, or the forms of war. What we are referring to is the function of warfare.

Qiao and Wang, Unrestricted Warfare

In their 1999 publication of *Unrestricted Warfare*, Colonels Qiao Liang and Wang Xiangsui of the Chinese People's Liberation Army (PLA) outline the changing function of warfare and prescribe a multitude of means that could be used to effectively strike the United States. In June 1999, in an interview with the PLA party youth league's official daily *Zhonggu Qingnian Bao*, Qiao is quoted as saying that, "the first rule of unrestricted warfare is that there are no rules, with nothing forbidden."[3] Qiao and Wang advocate a multitude of means, military and particularly non-military, to accomplish national ends. They emphasize that there is a clear distinction in mindset between strong countries and weaker countries in the way they conduct warfare. They maintain that strong countries make up the rules—and change the rules to suit their interests—and therefore are predisposed to abide by those rules, while weaker, imposed-upon countries (or non-state actors) have far less to lose by breaking those rules. They even propose a "secret to success." In chapter four they write: "All of the opponents who have engaged in battle with the American military have probably mastered the secret of success—if you have no way of defeating this force, you should kill its rank and file soldiers."[4] Here, the two PLA colonels also stress the fact that American society and its military have become so sensitized to human casualties that reducing casualties and achieving war objectives have become equal in weight on the U.S. priority scale.[5] Is this perception of a restrained mindset the reality?

Qiao and Wang boldly amend Carl Von Clausewitz's "destructive principle" wherein he emphasized that the dominant consideration is the exclusive destruction of the enemy military.[6] Rather, they assert that the age of technological integration and globalization has re-ordered not only the relationship of weapons to war (means) but more importantly the relationship of targeting to war (ways). In other words, the target is no longer restricted to the military component but to all other sectors of the enemy society. The emphasis is not so much on the means as it is on the results and ways to achieve the results. The argument seems to be characterized by effects-based thinking. Consequently, they state that economic attacks, terrorist attacks, or chemical-biological-radiological attacks on the adversary's populace and infrastructure, no matter how small in scale, have effects whose "degree of destruction is by no means second to that of war…[and] …represent semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare."[7] What once may never have been considered legitimate war actions can now yield warlike effects. In short, this new mindset transcends "conventional" boundaries and expands the battlespace into areas that were never anticipated, thus disregarding the so-called rules of war.

To say a significant portion of the world does not share in the West's idea of *jus in belli* (just conduct in war) or in the idea of *jus ad bellum* (the just war) is an understatement. If one does not acknowledge that the basis of differences in warfighting thinking lie, in part, in cultural differences, then one fools oneself. To understand fully the scope of a possible enemy mindset, it is requisite that one undertakes the responsibility to gain an appreciation of that culture—politically, historically, religiously, and otherwise. The current technological orientation of the Western mind, along with the assumed universality of Western values, distorts the analysis of an adversary's means and objectives.[8] The current U.S. mindset is

prone to asymmetrical vulnerabilities, for it assumes that our enemies will follow the established Western guidelines for the conduct of war. Until that mindset is altered to view the enemy and the battlespace in this very different context, the asymmetric comparative advantage will not be on the side of the U.S. military.

While the United States does its supposed rational calculus, and perceives its comparative advantage against its adversaries in technological terms, our enemies quantify *their* comparative advantage in possibly quite a different manner. For example, the emphasis on ethical standards, humanitarian concerns, and political realities of a capitalistic democracy are part of the Western value system that can be exploited as vulnerabilities by an adversary. This has been demonstrated in recent conflicts where non-combatants were chained to known targeted military sites, or by the military use of traditionally off-limits locations, such as mosques, to deter attack. No matter how stealthy the aircraft or how accurate the bomb, the U.S. military today will not knowingly target friendly forces or bomb a mosque in order to achieve military objectives. In short, some of the asymmetric strategies that the enemy may choose are not designed to defeat U.S. military forces but rather to erode at the U.S. political support from its population, coalition members, and within the arena of international opinion. In these examples, the enemy has not only eroded the effectiveness of our military capabilities, but has limited our capacity by virtue of our own rule sets via the concept of *jus in belli.*

III
THE THREAT

Now shadowy networks of individuals can bring great chaos and suffering to our shores for less than it costs to purchase a single tank...The gravest danger our nation faces lies at the crossroads of radicalism and technology... America is now threatened less by conquering states than we are by failing ones.

George W. Bush, National Security Strategy 2002

At this juncture, it is important to note that, for purpose of narrowing the scope of this analysis, the remainder of this paper will be in reference to the most dangerous threat—the rogue state, the failed state, and the non-state actor. A state is defined as having territorial boundaries, a formal structure of governance, and legal sovereignty.[9] A "rogue state" is a state that is in breach of established international norms and agreements or is not guided by the accepted international principles. The most obvious examples of this category are Iraq, Iran, and North Korea—the Commander-in-Chief's "axis of evil." On the other hand, a state is considered a failing state if it does not possess the abilities and does not fulfill the obligations of statehood.[10] Because the failed state does not have the wherewithal to compel internal order, it is susceptible to the influence of the so-called "Super-Empowered-Individual"[11] or non-state actor. What these three—the rogue state, the failed state, and the non-state actor—have in common with respect to the use of asymmetric warfare is that they have the greatest tendency to employ asymmetric strategies. Additionally, it is very probable that Super-Empowered Individuals, non-state actors, failed states, and rogue states have similar objectives with respect to that which they see as their enemy.

Usama Bin Laden (UBL) is one such example, where a Super-Empowered-Individual with ties to many terrorist organizations (Al Qaeda, Al Jihad, Harakat ul-Ansar, Gamaa Islamiya),[12] failed states (Afghanistan, Somalia)[13], and a rogue state (Sudan)[14] has staged and launched a series of operations and major operations based primarily on asymmetric

strategies. APPENDIX A lists chronologically the attacks in which UBL has either claimed responsibility or has been implicated as the alleged mastermind, financier, or has provided logistical or training support. The point is that UBL's operations have spanned a decade and promise to continue in scope and magnitude. Yet, Bin Laden is still unaccounted for, and his terrorist networks have continued to leverage "combat power."

Current conventional U.S. military capability lacks the "skill sets" to deal with this future asymmetric threat typology effectively. In the absence of a pervasive human intelligence network, this threat is extremely hard to detect.[15] The intelligence network necessary to perform the necessary functions resides primarily in the governmental civilian sectors where it is, today, being synthesized within the Department of Homeland Security (DHS). Is the military instrument of power really "dead in the water" when it comes to combating the adversary using asymmetric strategies? No. The continuing effort in Afghanistan is proof that the U.S. military is having success—but it is limited. One could argue that it is limited because the attack on the United States was not averted in the first place. Limited because the perpetrators have not all been brought to justice. This does not meet the criteria for winning the war against any adversary—conventional or not. Perhaps the ultimate measure of success against an adversary using asymmetric strategies is prevention.

IV
TECHNOLOGY

No degree of technological development or scientific calculation will diminish the human dimension in war. Any doctrine which attempts to reduce warfare to ratios of forces, weapons, and equipment neglects the impact of the human will on the conduct of war and is therefore inherently flawed.

MCDP-1 WARFIGHTING

With respect to the fielded and developing weapons systems and platforms or "tools" and processes designed to deal with the conventional threat paradigm, the U.S. military has a commanding lead and continues to expand a technological gap that will not be closed in the foreseeable future. Most estimates claim that this period will not be less than fifteen years. Not only has this technological gap become a hindrance vis-à-vis interoperability concerns with allies, it has potentially become a critical vulnerability vis-à-vis a potential adversary. While the United States is "making the weapons that fit the fight," our potential adversaries seek to "fight the fight that fits their weapons."[16] At first look, it would seem fairly obvious that the former phrase has more positive connotations, while the latter would seem to be reactionary. However, this concept contains two distinct schools of thought. On second look, the aspect of "making the weapons that fit the fight" lends itself to heavy reliance on technological advances, upon which one bases warfighting capabilities. A modern day example is the initiative of U.S. "network-centric warfare" (NCW)—a concept based primarily on the supposedly overwhelming advantages of information dominance and dispersed "netted" forces, whereby the networked forces achieve a major increase in combat power. This technologically-based initiative is one wherein the "net" can be seen as a center of gravity (COG).[17] But, system weaknesses can cause the net to be unhinged, neutralized, or can otherwise negatively affect it, creating a critical vulnerability (CV). In essence, an enemy does not have to defeat such a net in its entirety; simply targeting critical nodes and

links to the appendages of the network can render those elements ineffective and "de-linked."[18] Given this situation, a weakened or disabled "net" can cause the balance of combat power to quickly shift to the enemy.

On the other hand, due to the overwhelming supremacy of U.S. conventional weapon capabilities, and because of their own fiscal constraints and increasing technological inadequacy, adversaries "fighting the fight that fits their weapons" adapt and optimize the means at their disposal and seek new ways to engage. From the enemy perspective, the gap between U.S. technological sophistication and that of its own capability can be referred to as "asymmetric maneuver space." In fact, the greater the gap between U.S. technological superiority and that of a potential adversary, the greater the potential for the use of asymmetric strategies in this "asymmetric maneuver space." That is, as individual weapons systems, platforms, and personnel become more expensive to develop, train, and maintain, enemy actions resulting in loss of even a small amount of that capability may disproportionately affect our ability to leverage combat power. One example is the attack on the U.S.S. Cole in a Yemeni port. The reaction to this tactic has been an emphasis on the primacy of force protection around the globe for U.S. military forces and fielded weapons platforms. Hence, a U.S. Navy ship and its embarked combatants pulling into a port abroad today are often at a higher state of alert than is routine during some conventionally threatening situations. The operative word in the passage just described is "reaction." Such a position is not tenable in an asymmetric battlespace.

In light of the old and new threat paradigms, the U.S. "toolbox" must retain the conventional capabilities while at the same time developing those capabilities that deny the enemy "asymmetric maneuver space." With this base of logic, the conclusion would be that

those at the deficit end of the technological continuum (e.g., the rogue state, the failed state, and the non-state actor) have the most potential for the use of asymmetric strategies. An adequate amount of emphasis must be placed on the asymmetric threat paradigm, for it is today the most dangerous enemy course of action (ECOA). COCOMs must reshape their ability to leverage combat power to mirror the challenges at hand. Since it is unlikely that all attempts of an adversary using asymmetric strategies can be prevented, then perhaps the achievable measure of success against these strategies is protection.

V
OPERATING BEYOND THE "BOX"

To defeat this threat we must make use of every tool in our arsenal…we must be prepared to defeat our enemies' plans, using the best intelligence and proceeding with deliberation,…the only path…is the path of action.

George W. Bush, National Security Strategy 2002

Operational capability is defined as the ability to react to a changing situation and external stimulation of an assigned mission; it depends primarily on the number and structure of subordinate elements and the scheme connecting those elements.[19] Among the highest priorities of the operational leader is the ability to effectively and efficiently husband and project operational capability in the form of combat power in order to bring the enemy to an early culminating point. Professor Milan Vego defines combat power as, "the actual capability of a force generated in the course of mission accomplishment against a given enemy force."[20] Expanding on that definition, combat power is really *relative* to the enemy since it cannot be ascertained until it is viewed with respect to the enemy within the environment and situation in which it is to be leveraged. Combat power is thus measured in terms of whether it is sufficient to accomplish the mission.[21] That is, if the enemy can not be identified, located, and fixed, what effect do arsenals of laser-guided and GPS-guided bombs have? The question at the heart of this analysis deals with whether the COCOM has the necessary "tools and skill sets" in the toolbox to decisively win against the state and non-state adversary employing asymmetric strategies.

The case argued herein is that operational commanders take a harder look at the emerging threat paradigm and examine their "threat response." What are some responses that could best be used against the asymmetric adversary? One could argue that they are probably varied. Is the approach of the usual response—conventional military power—the best response? Although effective, this approach is very limited, particularly since the

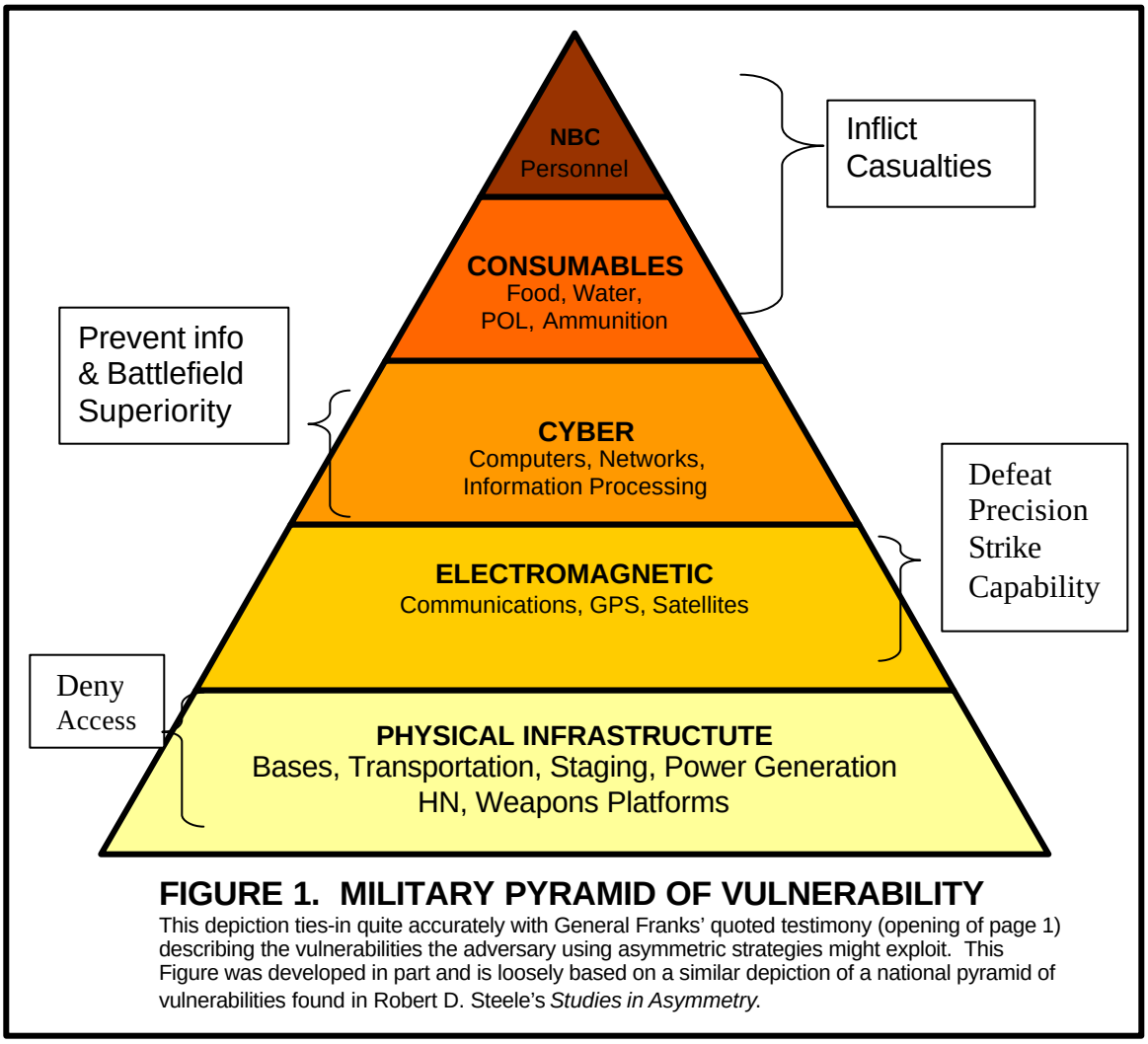

FIGURE 1. MILITARY PYRAMID OF VULNERABILITY

This depiction ties-in quite accurately with General Franks' quoted testimony (opening of page 1) describing the vulnerabilities the adversary using asymmetric strategies might exploit. This Figure was developed in part and is loosely based on a similar depiction of a national pyramid of vulnerabilities found in Robert D. Steele's *Studies in Asymmetry.*

calculating adversary knows our conventional "playbook" and has no intention of engaging the U.S. military force-on-force. A response that could be employed against such an adversary could be based on three pillars: prevention, protection, and pro-action.

The First pillar is prevention. The U.S. military has and needs to continue to prevent the successful employment of asymmetric strategies. FIGURE 1 shows a pyramid of key U.S. military vulnerabilities. Prevention of the successful targeting of these vulnerabilities is

paramount. Intelligence efforts across the spectrum of capabilities from open-source to HUMINT to high-technology networks can provide a decisive advantage in prevention.

The second pillar is protection. This concept concedes to enemy action, but seeks to limit its effectiveness. This is an idea of "fire-walling" against enemy efforts which would serve to limit the adversary's capability to the greatest extent possible. There needs to be redundant and alternate methods of operability if enemy asymmetric tactics cannot be prevented. Initiatives must be taken to insure that there are no "single point of failure" nodes within the warfighting network. An example would be the devastating effect of a successful enemy attack on the operability of our Global Positioning System (GPS) or our extensive network of information systems—both technology-induced vulnerabilities.

The third and last pillar is pro-action. The operational commander must "take the path of action" and formulate lethal offensively-minded strategies that attack the enemy's plans deliberately. Though the first and second threat responses above are passive measures and the third is an active measure, all serve to "shrink" the enemy's "asymmetric maneuver space." While the first two responses may prevent the successful use of an enemy asymmetric strategy, they do not cause the enemy to be defeated. It is the third response that will allow the U.S. military to win against the adversary using asymmetric strategies—the next focal point of this analysis.

What are the "other instruments" that the COCOM can combine with the existing ones? The instruments whose application is being recommended here already exist. They reside within the U.S. governmental civilian communities. The operational commander's staff organization should include and fully integrate into its planning processes those governmental and civilian agencies that possess the high value skill sets necessary. These

skill sets could be focused to formulate asymmetric strategies. The capabilities that these agencies contribute, such as information collection, military and other types of intelligence, analysis, and processing are crucial for the operational commander's estimate of the situation. Those agencies include the FBI, CIA, DEA, NIMA, INS, etc. In addition to intelligence analysts, collectors, and processors, the necessary skill sets should also include cultural and religious experts, cyber experts, regional experts, chem-bio experts, linguists, geo-political experts, and any field of expertise that could be relevant. The proposal is that these "skill sets" be "fused" in a permanent staff at the operational level—a staff that will assist the commander by providing specialized expertise for the formulation of asymmetric strategies. This fused staff can be referred to as a "Black Cell."

The Black Cell's *raison d'être* would be to formulate asymmetric strategies to exploit the critical vulnerabilities leading to the defeat of the center(s) of gravity of the enemy. This cell would support the operational commander directly in taking advantage of new warfighting concepts based upon asymmetric strategies. The strategies would focus on the enemy's cultural infrastructure, cyber infrastructure, and information infrastructure—to name a few. These strategies would vary from adversary to adversary, since the "asymmetric maneuver space" they would seek to operate in is representative of the "delta" between friendly and enemy capabilities. Formulating effective strategy is the bridge between understanding the asymmetric threat and structuring (or shaping) the force to win.[22] This planning cell would operate in close coordination with the J2 and the J3. Knowledge of the enemy—culturally, religiously, politically, economically, socially, militarily, technically, etc., would be key considerations in formulating a winning strategy at the operational level.

The nature of this concept is offensive. It is not a "Red Cell," nor is it the "OpFor" (opposition forces). A red cell is a planning cell that, based on known enemy doctrine and templates, provides improved knowledge of enemy capabilities and tactics, while the OpFor is the force that employs those tactics and capabilities during training exercises against the designated friendly (or Blue) forces. On the contrary, the "Black Cell" would focus on attacking an adversary "asymmetrically," with much greater latitude than that afforded to conventional forces—or even Special Operations Forces. The specific task organization (TO) of such a cell would be driven by the regional demands within a particular COCOM. This staff would consist of civil-military experts synchronized in effort and scope.

This "fusion" of civil-military experts is not an advisory element that *represents* the various civilian departments and agencies in order to facilitate information sharing across interagency communities. That is the description of the Joint Interagency Coordination Group (JIACG).[23] The JIACG concept seeks to establish operational connections between civilian and military departments and agencies that will improve planning and coordination. Rather, the proposed "Black Cell" would be *organic* to the COCOM TO. This cell would formulate asymmetric strategy using very different criteria than that used by a conventional planning cell. Concepts such as mass, objective, offensive, surprise, economy of force/effort, maneuver, unity of command, simplicity, and security (MOOSEMUSS) could be replaced with other—still to be determined—concepts.

In *Unrestricted Warfare*, Qiao and Wang offer the following principles: omni-directionality, synchrony, limited objectives, unlimited measures, asymmetry, minimal consumption, multidimensional coordination, and adjustment and control of the entire process. A summarized description of each can be found in Appendix B. With these

principles in mind, one can more readily appreciate the definition of asymmetric warfare arrived at in the introduction of this analysis. Regardless of the specific terms (or ensuing acronym) used as principles of asymmetric warfare, the engine that drives these concepts is the mindset. A mindset that understands that use of the normal force is to engage but use of the extraordinary is to win.[24]

VI
CONCLUSION

And as water shapes its flows in accordance with the ground, so an army manages its victory in accordance with the situation of the enemy. And as water has no constant form, there are in war no constant conditions. Thus, one is able to gain victory by modifying his tactics in accordance with the enemy situation may be said to be divine.

Sun Tzu, The Art of War

The terrorist attacks on September 11, 2001 have raised fundamental questions concerning one of the most basic obligations of a state—that of protecting its citizenry, territory, and resources.[25] The perpetrators are described as a "shadowy network of individuals." Despite the overwhelming technological superiority of the United States, the emergence of the Super-Empowered-Individual has prompted an unparalleled re-organization within key U.S. institutions in unprecedented fashion. Since necessity is the mother of all invention, it has prompted substantial reconstruction of the nation's domestic security posture resulting in the Department of Homeland Security (DHS). The lead agency/agencies within the DHS will be the one(s) best equipped to collect, coordinate, analyze, and process information. The U.S. military and other institutions will be in a supporting position to those civilian elements. Likewise, civilian agency support to Department of Defense (DOD), or more specifically the COCOM, will be vital.

In his 2002 National Security Strategy, the Commander-in-Chief has asked for "a wider range of military options."[26] The challenge will be to maintain dominance over "shadowy networks of individuals" and failed or rogue states using asymmetric strategies as well as those who seek to challenge the U.S. military in the conventional realm. But, because of U.S. dominance in conventional warfare, the future adversary is even more likely to fight using asymmetric strategies. This is a by-product of success and a result of the law of

unintended consequences. The force-on-force conventional war planned for since the end of WWII will be the atypical war in the future.

Nevertheless, the U.S. military must be prepared for adversaries across the spectrum of warfare in the 21st century battlespace. A combination of conventional and asymmetric options and expertise ("tools" and "skill sets") must be employed when considering future warfare along the whole spectrum of conflict. The U.S. military instrument of power must explore and plan threat responses that can be combined with existing capabilities. An asymmetric warfare mindset can be used with telling effect in theater wars, small scale contingencies, and against the non-state actor. This is consistent with the idea of Full Spectrum Dominance—a responsibility of the COCOM.[27]

The three pillars of prevention, protection, and pro-action are offered as possible essential elements of a threat response strategy. The recommendation of a "Black Cell" is just one of many initiatives that could be employed to effectively deal with the enemy on asymmetric battlespace. The function of the military instrument of power is to fight and win. If the enemy operates "outside the box," then the overarching mission of the U.S. military is to "fight and win outside the box."

APPENDIX A

DATE	EVENT	LOCATION	REMARKS
DEC 1992	ATTEMPTED BOMBING OF TWO HOTELS	ADEN, YEMEN	100 US MILITARY TARGETED 3 KILLED (NOT US)
FEB 1993	BOMBING WORLD TRADE CENTER	NEW YORK, NY	6 KILLED >1000 WOUNDED
OCT 1993	GUERILLA ASSAULT	SOMALIA	18 US KILLED
NOV 1995	BOMBING OF MILITARY COMPLEX	RIYADH, SAUDI ARABIA	7 KILLED (5 US) 60 WOUNDED
JUN 1996	BOMBING OF KOBAR TOWERS	DHARAN, SAUDI ARABIA	19 US SOLDIERS KILLED 500 WOUNDED
AUG 1998	BOMBING OF US EMBASSY	NAIROBI, KENYA DAR ES SALEM, TANZANIA	224 KILLED 5000 WOUNDED
JAN 2000	ATTEMPTED ATTACK OF NAVY VESSEL	ADEN, YEMEN	US MILITARY TARGETED
OCT 2000	BOMBING OF USS COLE	ADEN,YEMEN	17 US KILLED 39 WOUNDED
SEP 2001	DESTRUCTION OF WTC ATTACK ON PENTAGON	NEW YORK, NY WASHINGTON, DC	>3000 KILLED
OCT 2002	BOMBING OF BAR/CLUB	KUTA BEACH, BALI	193 KILLED 132 WOUNDED

Claimed responsibility **Implicated**

The above lists attacks in which Usama Bin Laden has either claimed responsibility or has been implicated as either a mastermind, financier, or as having provided combatant training support. This table is compiled from The Washington Post database website and the Reuters news service.

APPENDIX B

QIAO AND WANG'S SUMMARIZED UNRESTRICTED WARFARE PRINCIPLES	
OMNI-DIRECTIONALITY	The starting point of "unrestricted warfare" ideology. To give all-round consideration to all factors related to "this particular" war. When observing the battlefield or potential battlefield, designing plans, employment measures, combining all war resources that can be mobilized, to have a field of vision with no blind spots, a concept unhindered by obstacles, and an orientation with no blind angles.
SYNCHRONY	Key factors of warfare which are dispersed in different spaces and domains to bear in the same designated space of time. Synchrony is not simultaneity, but rather "within the same time period"; it is "designated time warfare." Technical measures employed in modern warfare and the spread of information technology; the emergence of long-range warfare technology; increased ability to transform the battlefield; the linking together of battlefields which stretch forever, are scattered, or are different by nature; and the introduction of various military and non-military forces on an equal footing in war—all these greatly shrink the course of warfare. The stress on "synchrony" in combat exceeds the stress on "phasing." Emphasis on expansion to battlefields beyond the military sphere.
LIMITED OBJECTIVES	Limited in relation to measures used. Objectives must always be smaller than measures. Give full consideration to feasibility of accomplishing the objective. Do not pursue objectives which are unrestricted in time and space. After accomplishing an objective, one will have the resilience to pursue the next. Overcome the mentality of craving great successes, instead pursue limited objectives and eliminate objectives which are beyond abilities.
UNLIMITED MEASURES	Unlimited measures are related to limited objectives. Measures are inseparable from objectives. Employ measures (range, selection, and methods) beyond restrictions and boundaries to accomplish limited objectives. The measures cannot go beyond the objective. Atomic weapons, which can annihilate mankind, have been viewed as absolute measures precisely because they violate the principle that a measure must be used to accomplish an objective.
ASYMMETRY	Follow the train of thought opposite to the balance of symmetry and develop combat action on that line. From force disposition and employment, selection of main combat axis and the center of gravity for the attack, all the way to the allocation of weapons; in all these, give two-way consideration to the effect of asymmetrical factors, and use asymmetry as a measure to accomplish the mission. Understanding and employing the principle of asymmetry correctly allows us to find and exploit an enemy's soft spot. The resultant of such action is a huge psychological shock to an adversary.
MINIMAL CONSUMPTION	Use the least amount of combat resources sufficient to accomplish the mission. First, rationality is more important than thrift; second, the size of combat consumption is decided by the form of combat; and third, use "more" measures to pursue "less" consumption. Combine the superiorities of several kinds of combat resources in several kinds of areas to form a completely new form of combat, accomplishing the objective while at the same time minimizing consumption. "Minimal consumption" is to find a combat method which makes rational use of combat resources. The result of a mismatch between measures and objectives is inevitably high consumption and low effectiveness.
MULTI-DIMENTIONAL COORDINATION	Coordinating and allocating all the forces which can be mobilized in the military and non-military spheres covering an objective. Another way of saying multiple spheres and multiple forces. Refers to cooperation among different forces in different spheres, not in the sense of mathematics or physics. The great difference here from the conventional meaning is in the introduction on non-military and non-war factors into the sphere of war directly rather than indirectly. Since any sphere can be a battlefield, and any force can be used under combat conditions, this principle is the coordination of the military dimension with various other dimensions. It is not the case that military action be considered the primary form of action. Future warfare is equalizing the various dimensions in war. Pay particular attention to the employment of intangible "strategic resources" such as geographical factors, history, cultural traditions, ethnicity, and the influence of international organizations.
ADJUSTMENT AND CONTROL OF ENTIRE PROCESS	During the entire course of war, from its start, through its progress, to its conclusion, continually acquire information, adjust action, and control the situation. Warfare is a dynamic process of randomness and creativity; therefore, it is necessary to have feedback and revisions throughout in order to maintain the initiative. Technology has increased the factors and the speed of development of war. With this burst of technology and new measures, managing the process is becoming more of a skill; a skill requiring the greater use of intuition. The process must be controlled if one is to win.

NOTES

[1] Tommy R. Franks, "Statement," U.S. Congress, House, Armed Services Committee, Fiscal 2003 Defense Budget, Hearing before the Armed Services Committee, 107th Congress, 2d sess., 27 February 2003, 2.

[2] Lloyd J. Matthews, ed., Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated? (Pennsylvania: Strategic Studies Institute, 1998), 87.

[3] Qiao Liang and Wang Xiangsui, Unrestricted Warfare, trans. FBIS (Beijing: PLA Literature and Arts Publishing House, 1999), 2.

[4] Qiao and Wang, 93.

[5] Ibid, 93.

[6] Carl von Clausewitz, On War, trans. and ed. Michael Howard and Peter Paret (Princeton: Princeton University Press), 228.

[7] Qiao and Wang, 6.

[8] Matthews, 5.

[9] Douglas H. Dearth, Failed States: An International Conundrum (McLean, VA: Joint Military Intelligence College Foundation, 1996; reprint, Newport, RI: U.S. Naval War College), 120 (page citation is to the reprint edition).

[10] Ibid, 121.

[11] Thomas P. M. Barnett and Arthur K. Cebrowski, "The American Way of War," U.S. Naval Institute Proceedings (January 2003): 42-43.

[12] "World Terrorist Attacks and Organizations: Osama Bin Laden," The Washington Post Online, <http:www.washingtonpost.com/ac3/ContentServer?node=world/issues/terrordata&pagename=world/terror> [21 January 2003].

[13] Walter H. Kansteiner, "Statement," U.S. Congress, Senate, Foreign Relations Subcommittee on African Affairs, Weak States and Terrorism in Africa: U.S. Policy Options in Somalia, 107th Congress, 2d sess., 6 February, 2002.

[14] "World Terrorist Attacks and Organizations: Sudan," The Washington Post Online, <http:www.washingtonpost.com/ac3/ContentServer?node=world/issues/terrordata&pagename=world/terror> [21 January 2003].

[15] Robert D. Steele, "The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats," Studies in Asymmetry, Strategic Studies Institute (U.S. Army war College, 2002), 9.

[16] Qiao and Wang, 19.

[17] Headquarters Marine Corps, War Room Report 2-03, (Washington, D.C.: 2003), 1.

[18] Ibid, 1.

[19] Milan N. Vego, Operational Warfare (Newport: Naval War College, 2000), 640.

[20] Ibid, 634.

[21] Headquarters Marine Corps, War Room Report 3-03, (Washington, D.C.: 2003), 1.

[22] Steele, 6.

[23] "Joint Interagency Coordination Group," United States Joint Forces Command, <http://www.jfcom.mil/about/fact_jiacg.htm> [30 January 2003].

[24] Sun Tsu, The Art of War, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1963), 91.

[25] Dearth, 121.

[26] U.S. President. Document. 2002 National Security Strategy. 30.

[27] Headquarters Marine Corps, War Room Report 3-03, 1.

SELECTED BIBLIOGRAPHY

Barnett, Thomas P. M. and Arthur K. Cebrowski. "The American Way of War." U.S. Naval Institute Proceedings (January 2003): 42-43.

CJCSI 3121.01A Instruction. Standing Rules of Engagement for U.S. Forces. Washington, D.C.: Chairman of the Joint Chief of Staff, 2000. Reprint, RI: U.S. Naval War College.

Cline II, Donald L. "Does the Theater Commander Really Know the Enemy: A Case for the Standing Theater 'Red Cell'." Unpublished Research Paper, US Naval War College, Newport Rhode Island, 2000.

Dearth, Douglas H. Failed States: An International Conundrum. VA: Joint Military Intelligence College Foundation, 1996. Reprint, RI: U.S. Naval War College.

"Joint Interagency Coordination Group." United States Joint Forces Command. <http://www.jfcom.mil/about/fact_jiacg.htm> [30 January 2003].

Lwin, Michael R. "Great powers Weak States and Asymmetric Strategies." Unpublished Research Paper, Naval Post Graduate School, Monterey, California, 1997.

Matthews, Lloyd J., ed. Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?. Pennsylvania: Strategic Studies Institute, 1998.

McKeown, Wendell B., Information Operations: Countering the Asymmetric Threat to the United States. Carlisle, PA: U.S. Army War College, 1999.

Miles, Franklin B. "Asymmetric Warfare: An Historical Perspective." Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA. 1999.

Qiao Liang and Wang Xiangsui. Unrestricted Warfare. Translated by FBIS. Beijing: PLA Literature and Arts Publishing House, 1999.

Schmitt. M. N., ed. International Law Studies: The Law of Military Operations. Reprint, RI: U.S. Naval War College, 1998.

Staten, Clark L. Asymmetric Warfare, the Evolution and Devolution of Terrorism; The Coming Challenge for Emergency and National Security Forces. April 1998. <http://www.emergency.com/asymetrc.htm> [21January 2003].

Steele, Robert D. "The new Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats," Studies in Asymmetry. Strategic Studies Institute, U.S. Army war College, 2002.

_____. Takedown: The Asymmetric Threat to the Nation. June 1998. <http://www.defensedaily.com/reports/takedown.htm > [30 January 2003].

Sun Tzu. The Art of War. Translated by Samuel B. Griffith. Oxford: Oxford University Press, 1963.

Tucker, Jonathan B. Asymmetric Warfare: An emerging Threat to U.S. Security. May 1997. <http://www.comw.org/qdr/tucker.htm> (2 January 2003)

U.S. Congress. House. Armed Services Committee. Fiscal 2003 Defense Budget: Hearing before the Armed Services Committee. 107th Cong, 2d sess., 27 February 2003.

U.S. Congress. Senate. Foreign Relations Subcommittee on African Affairs. Weak States and Terrorism in Africa: U.S. Policy Options in Somalia: Testimony before the Foreign Relations Subcommittee on African Affairs. 107th Congress, 2d sess., 6 February, 2002.

U.S. Department of Defense. Joint Pub 2-0: Doctrine for Joint Operations. Washington D.C.: Department of Defense, 1996.

_____. Joint Pub 3-08: Interagency Coordination during Joint Operations, Vol I. Washington D.C.: Department of Defense, 1996.

_____. Joint Pub 3-08: Interagency Coordination during Joint Operations, Vol II. Washington D.C.: Department of Defense, 1996.

_____. Joint Pub 5-00.2: Joint Task Force Planning Guidance and Procedures. Washington D.C.: Department of Defense, 1999.

U.S. Marine Corps Headquarters. War Room Report 43-02. Washington, D.C.: 2002.

_____. War Room Report 47-02. Washington, D.C.: 2002.

_____. War Room Report 2-03. Washington, D.C.: 2003.

_____. War Room Report 3-03. Washington, D.C.: 2003.

U.S. Navy Department. Naval Power 21: A Naval Vision. Washington, D.C.: 2002.

U.S. President. Document. National Security Strategy. Washington, D.C. 2002.

Vego, Milan N. Operational Warfare. Newport: Naval War College, 2000.

Von Clausewitz, Carl. On War, Translated and edited By Michael Howard and Peter Paret. Princeton: Princeton University Press.

"World Terrorist Attacks and Organizations: Osama Bin Laden." The Washington Post Online.<http:www.washingtonpost.com/ac3/ContentServer?node=world/issues/terror data &pagename=world/terror> [21 January 2003].

"World Terrorist Attacks and Organizations: Sudan," The Washington Post Online, <http:www.washingtonpost.com/ac3/ContentServer?node=world/issues/terror data&pagename=world/terror> [21 January 2003].

Wurzel, Donald J., and Kenneth R. McGruther and William Murray. A Survey of Unclassified Literature on the Subject of Asymmetric Warfare. Sherman Oaks, CA: Arete Associates, 1998.