A New Kind of War: Adaptive Threat Doctrine and Information Operations

A Monograph

by

Major Paul S. Warren

United States Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

First Term AY 00-01

ABSTRACT

A NEW KIND OF WAR: ADAPTIVE THREAT DOCTRINE AND INFORMATION OPERATIONS by MAJ Paul S. Warren, USA, 46 pages.

The United States military remains the dominant post-modern state combatant. Military actions in Kosovo, Bosnia, and the Desert Storm victory validated the theory that information-based technologies are decisive factors in modern military operations. Threats recognize that peer competitors of the U.S. do not exist and are several decades away from developing similar military technologies. Consequently, threat-based strategies seek alternative or asymmetrical methods of warfare designed to exploit U.S. weaknesses and disrupt or paralyze the decision-making apparatus.

Information operations provide opportunities to avoid direct contact with superior conventional forces and threat capabilities enhanced where qualitative gaps with opposing forces exist. The theoretical framework for the study is a model of information warfare that draws a distinction between "cyberwar" and "netwar," two components of information warfare that are structurally different. Using a hybrid of this model, the effectiveness of threat strategy using "netwar" to disrupt the decision-making process and create paralysis at the strategic and operational level can be determined.

Understanding how the threat is adapting to knowledge-based warfare and U.S. military information dominance is vital to U.S. national interests. What methods are state and non-state actors using to counter U.S. technological superiority? Can adaptive threat applications be developed that cause strategic and operational paralysis? If so, then are they successful in achieving threat end-states and are they designed to use information operations to gain a relative advantage? Can it be shown that future threats to the security of the United States can develop new ways, specifically "netwar" strategies, to attack and exploit U.S. military weaknesses?

Conclusively, threats to the security of the United States and her allies might achieve the operational and strategic paralysis of U.S. and allied military forces through "netwar strategies." The leveling effect of the information revolution reduces the barriers of entry to threat states and organizations. The distributed and nondescript nature of the world-wide-web allows states and non-state actors with agendas that threaten regional stability to become difficult to counter and assign accountability. The likely implications for the future are, first, the information revolution will continue to favor networked organizations with flat command and control structures. Second, highly automated and hierarchical systems such as the U.S. will become more vulnerable to disruption from directed informational flows that seek to overload sensors and collection assets. Finally, it takes networks to fight networks. The future may require new organizations that are a hybrid of military units and non-military organizations working in conjunction to locate and counter networked threats.

TABLE OF CONTENTS

CHAPTER 1

Introduction

The nature of warfare has changed dramatically since the end of the Cold War. Conventional forces that are smaller, more agile, and possess greater lethality characterize the battlefield today. Post-industrial age technology allows states to project force globally in a short amount of time. Images of modern conflict portray military forces gaining relative advantage on the battlefield through dominant maneuver supported by information superiority and precision strikes at enemy centers of gravity.

The Desert Storm victory validated the emergence of a technologically superior United States military as the dominant post-modern state combatant. Further validated was the notion that knowledge-based warfare will define the spectrum of conflict for the next century and that information-based operations are decisive factors in modern military operations. Current lexicon describes this as a "revolution in military affairs" or RMA. Yet, as with all revolutions in warfare, history suggests that adaptive threat strategies will occur to counter dominant military capabilities.

It is vital to U.S. national interests to understand how the threat is adapting to knowledge-based warfare and U.S. military information dominance. What methods are state and non-state actors using to counter U.S. technological superiority? Can adaptive threat applications be developed that cause strategic and operational paralysis? If so, then are they successful in achieving threat end-states and are they designed to use information operations to gain a relative advantage? Can it be shown that future threats to the security of the United States can develop new ways, specifically "netwar" strategies, to attack and exploit U.S. military weaknesses?

Methodology and Research Design

A conceptual template will be established herein to describe conflict in the next century. The starting point for this discussion is the theoretical work of Samuel P. Huntington, Alvin and

Heidi Toffler, and Robert D. Kaplan. The usefulness of each of their theories on the nature of the post-Cold War environment is articulated in each author's concept of why conflict occurs and what factors contribute to its makeup. The inherent value of briefly examining each theory is to develop the notion that future threats to American security will not always take on the traditional form of a nation-state vs. nation-state. Future threats could very well be transnational actors as well as hybrids of state and non-state organizations capable of creating strategic and operational paralysis when confronted by U.S. military force.

The discussion will also confirm that, despite U.S. military dominance, American civilian and military decision-making apparatus are vulnerable to a range of information generated threats. Our opponents recognize that without adapting to counter the information and technological superiority of U.S. forces, winning on the battlefield is a remote possibility. The start point for understanding threat adaptation is to look at how the U.S. military is transforming its force for the future, specifically through the application of information technologies and doctrinal changes addressing the use of information operations to wage information warfare.

Drawing a distinction between "cyberwar" and "netwar" is critical to understanding how the enemy is adapting to the use of militarily superior forces across the spectrum of conflict. The focus is to validate that netwar as an adaptive measure, is capable of creating strategic and operational paralysis. A specific set of enablers that includes the use of off-the-shelf technologies such as communication, low cost computing technologies, the use of perception management, and access to western media sources and transnational actors enhance the ability of threat organizations to cause significant damage to western institutions.

By nature western democratic institutions are more vulnerable to netwar attacks because of open access to institutional structures and information. In many ways, the strength of western society is also a significant weakness in the information age. To demonstrate how netwar strategy is used, recent conflicts in Somalia, Kosovo, and the Zapatista insurrection in Mexico will be examined. Threat adaptation using netwar concepts in all three cases countered opponents

possessing superior military capabilities, creating a stalemate that preserved the institutional structure of each threat group.

Further discussion will assess how effective threat organizations are in achieving their objectives. Each case study mentioned in the preceding paragraph yields a unique outcome. It will be shown that netwar is used in various configurations designed to achieve a specific end-state, and that adaptation identifies threat organizations as learning organizations.

The final chapter will determine if the evidence and analysis presented supports the notion that adapting enemies represent a significant threat in the future. Is the trend for the next century of warfare centered on the innovative use of information and technology to construct a netwar capability to counter the application of U.S. and allied military power? If the assumption that adaptive threat strategies are a significant danger to military operations and create strategic and operational paralysis, then perhaps planning and organizational doctrine for future operations will require modification.

A Conceptual Framework for Future Conflict

The fundamental nature of war remains unchanged despite centuries of technological and tactical innovation. Clausewitz correctly warned that war… "is not the action of a living force upon a lifeless mass (total nonresistance would be no war at all), but always the collision of two living forces."[1] It is a highly complex interactive system characterized by friction, unpredictability, disorder, and fluidity, and not a mechanistic system subject to precise, positive control or synchronized schemes.[2] War remains an inherently human endeavor. However, how wars are waged and the dynamic environment in which they exist continues to change.

[1] Carl Von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1975), 86-87.
[2] Paul K. Van Riper, LTG USMC (Ret.) and E.G. Hoffman, LTC USMCR, "Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare." *NSSQ* (Summer, 1998), 5.

The 21st Century is no exception when attempting to predict how change will effect what the next war will look like or where and against whom it will be fought. Since the end of the Cold War a significant number of theories have emerged concerning future warfare. Samuel Huntington suggests future conflict will consist of civilizations pitted against each other, and concludes, "most important conflicts of the future will occur along cultural fault lines separating civilizations."[3]

In contrast, Alvin and Heidi Toffler argue that three distinct divisions (waves) of society exist in the world today and that as we move from one wave to the next the potential grows for increasing regularity and intensity of conflict.[4] The transition from agrarian-based to industrial and then to information-based structures creates a shock-effect that resonates across societal boundaries. Conflict between waveforms is the norm because of the shifting of power and wealth.

A third viewpoint from Robert Kaplan suggests that the future international environment will mirror that of anarchy. Kaplan bases his theory on the premise that many nation-states are descending into a state of anarchy and becoming ungovernable.[5] Regional disputes tend to occur over access to natural resources and the delineation of geographical, cultural and racial boundaries. Conflict is a contest between the societies that have wealth and power and those that do not, and there is the potential for these conflicts to spread beyond regional confines.

The viewpoints of Kaplan, Huntington, and the Tofflers provide a benchmark for understanding the structure of the post-Cold War environment and the events that shape how it will look in the future. Each theory is relevant to explaining the appearance of new threats that were previously held in check by the bipolar international order of the last half of the 20th Century.

---

[3] Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (NY: Simon and Schuster, 1996), 3-6.
[4] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993), 18-22.
[5] Robert D. Kaplan, *The Coming Anarchy* (New York: Random House, 2000), 174-175.

The trend is that developed states, primarily Western nations, no longer dominate the international environment. What emerges is a global construct consisting of three tiers: mature states that possess fully developed economic, political, and social institutions; transitional states that are in the process of developing competing institutional structures; and a collective of failed states that rely on humanitarian and peacekeeping assistance from the developed nations.

Each tier of the global system has states and non-state groups with varying degrees of military capabilities that may pose a potential threat to U.S. national interests and to the interests of our allies. Further complicating the problem is the appearance of institutions that are not organized along the traditional hierarchical lines of nation-state actors but retain some degree of capability to counter the projection of Western political, economic, and military power. Regardless of whether the U.S. and her allies are dominant global military powers, the emerging security environment is characterized more by ethnic conflict, states seeking to achieve regional hegemony, and a variety of networked sub-state and non-state actors such as terrorists, separatists, and international criminal organizations.[6]

Nation-states such as the U.S. will certainly remain the primary actors in the post-Cold War world, and states such as China, Iraq, and North Korea will continue to threaten regional stability and U.S. interests. However, destabilizing sub-state and transnational actors that demand increased levels of attention to mitigate the effects of regional conflict, fragmentation, and societal change will mark the new "bifurcated international environment."[7]

The challenge in the future for the U.S. and most of the developed world is how to respond to a bifurcated international environment and the potential for destabilization where U.S. and allied interests are at stake. The average American has already had a glimpse of what may be on the horizon. U.S. military power continues to be the instrument of choice for ending violence

[6] Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., eds. *War in the Information Age: New Challenges for U.S. Security Policy* (Washington: Brassey's, 1997), 3.
[7] Ibid., 11.

in regional hot spots such as Bosnia, Haiti, Somalia, and Kosovo. The consistent use of U.S. military power to restore stability to regions at risk illustrates the advantages gained by the application of new technologies and training to maintain a modern, capable force. Yet, there are vulnerabilities in the highly sophisticated hierarchical systems that characterize U.S. military organizations and operations.

Information, Technology, and the American Way of War

The American way of war is traditionally characterized by the use of overwhelming force and the search for a technological advantage.[8] Prior to the end of World War II, technology and the quality of U.S. military forces played less of a role in defense strategy than ensuring victory through the application of unending supplies of men and material. Not until Vietnam did defense strategists recognize that the quality gained through the development of superior technologies would become a decisive factor in the rise of the U.S. as a dominant military power.

The invasion of Panama in 1989 and victory in the Persian Gulf in 1991 reaffirmed this idea by validating the role of information and high technology in achieving dominance on the modern battlefield. A new paradigm emerged for winning quickly, the result of both the increasing accuracy and destructiveness of weaponry, and the ability to coordinate and control complex maneuver and logistics over great distances.[9]

Because of the information technology explosion, what has evolved over the course of the last decade is the view that the U.S. military is experiencing a RMA. The general definition of a RMA is a phenomenon occurring when a significant discontinuous increase in military capability is created by the innovative interaction of new operational concepts and organizational

[8] An in-depth study of how America fights is articulated by Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington: Indiana Univ. Press, 1977).
[9] John Arquilla, "The Strategic Implications of Information Dominance." *Strategic Review* (Summer, 1994), 25.

structures.[10] History suggests that enablers of any RMA are doctrinal innovation, technological development, and organizational change. It is within the context of the current RMA that the impact of information and knowledge-based technologies is significant.

The official vision of future war reflects the belief that "information superiority" will be the lifeblood of a postmodern military and the key to battlefield success.[11] To transform U.S. military capability, the so-called RMA must focus on the development of improved information and command and control capabilities that significantly enhance joint operations.[12] Theoretically, war will be waged by a "system of systems" connecting an array of space-based, ground-based, and air-based sensors that reduces or eliminates friction. Aided by decision-assistance technology, information superiority will enable U.S. commanders to strike enemy centers of gravity and decisive points with precision weapons at the right time.[13]

Joint Vision 2020 further expands the conceptual template for change by supporting the notion that transformation will yield a force that can achieve "full spectrum dominance" through the interdependent application of maneuver, precision engagement, focused logistics, and full dimensional protection.[14] Superior information and knowledge are the key enablers to maximize the four operational concepts listed above, implying that a shift is underway from traditional warfighting with its massed force and sequential operations towards warfighting that is focused on massed effects and simultaneous operations.

To capture the shift away from a traditional way of warfighting in favor of the application of advanced weapons systems and operational concepts that favor technology, U.S. military forces are developing doctrine that focuses on information operations (IO). The operational

---

[10] Van Riper and Hoffman, 2.
[11] William S. Cohen, *Report of the Quadrennial Defense Review* (Washington, DC: Department of Defense, 1997), Section 2.
[12] Ibid., Section 7.
[13] Stephen Metz, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare* (Carlisle, PA: Strategic Studies Institute, April 2000), 27-28.
[14] *Joint Vision 2020* (Washington, DC: Chairman of the Joint Chiefs of Staff, n.d.), 1-3.

concept of IO and the effective use of information to enhance military capabilities in the future are becoming dominant features of warfare. Although not new to warfare, information is one of the five elements of combat power, maneuver, firepower, leadership, protection, and information, driving the transition of U.S. and allied military forces from "industrial age warfare" to "information age warfare."

Before considering the impact of information operations within the spectrum of conflict, a conceptual framework for information warfare (IW) must be established. Field Manual (FM) 100-6, Information Operations defines information warfare as a range of actions taken during conflict to achieve information superiority over an adversary.[15] The Joint Staff more narrowly defines IW as actions that affect an opponent's information, information-based processes, information systems, and computer-based networks while protecting our own similar systems.[16]

The IO concept then becomes a component of information warfare and is a developed capability within the full range of military operations. IO is conducted by all forces prior to deployment and does not conclude until mission completion. As a battlefield operating system, IO is integrated both defensively and offensively to shape operations and provide opportunities for decisive actions. The real value of IO is measured by its effect on an opponent's ability to conduct military actions by denying critical information or disrupting his decision making process and operational tempo.[17]

How the commander uses IO to gain the advantage over an opponent is linked to a set of enablers that give him superior knowledge of the enemy and the battlefield in the form of "situational awareness" and "situational understanding." FM 3-0: Operations and FM 100-6 identify the enablers critical to successful execution of IO as military deception,

[15] *FM 100-6: Information Operations* (Washington, DC: Headquarters Department of the Army, 1996), 2-2.
[16] Ibid.
[17] *FM 3-0: Operations (DRAG Edition)* (Washington, DC: Headquarters Department of the Army, June 2000), 11-16.

counter-deception, operations security, physical security, electronic warfare, information assurance, physical destruction, psychological operations, counterpropanganda, counterintelligence, computer network attack, and the related activities of public affairs and civil-military operations.[18] Military forces that effectively integrate IO enablers into conventional operations gain relative advantage by disrupting the opponent's decision cycle. Disruption of the decision-making apparatus subsequently leads to operational paralysis rendering an opposing force incapable of continuing effective combat operations.

U.S. military doctrine continues to emphasize the capacity to kill with greater and greater efficiency.[19] Yet, recent indications suggest that a movement away from a firepower-centered approach to conflict resolution is occurring. Although the paralysis generated by firepower to threat command and control structures often leads to culmination, firepower-centric paralysis erodes over time. Hence threat organizations rarely desire to directly confront U.S. military power, as evidenced by recent small-scale contingencies and peacekeeping operations in the last decade.

Network-centric Warfare

The information-age conflict spectrum must be defined to further understand how information is changing the face of war. John Arquilla and David Ronfeldt, from the RAND Institute, offer insight by breaking information war into two subsets, "cyberwar" and "netwar."[20] What is termed "cyberwar is important at the military end, where the focus is normally on high-intensity conflict (HIC) and mid-intensity conflict (MRC), but 'netwar' will figure more prominent at the societal end, where the language is normally about low-intensity conflict (LIC)

[18] Ibid., 11-17 – 11-19.
[19] Major General Robert Scales, Jr., *Future Warfare* (Carlisle Barracks, PA: U.S. Strategic Studies Institute, May 1999), 6.
[20] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996), 3.

and operations other than war (OOTW)."[21] Netwar is a much broader concept and more descriptive of the type of information warfare that characterizes today's military operations that include peacekeeping and complex humanitarian emergencies.

Whereas cyberwar is often associated with conventional force-on-force military operations, netwar more commonly involves non-state actors and transnational organizations. Both terms support the theory that a transformation in the nature of warfare is underway. Thus, the greatest challenge confronting the U.S. is a more asymmetrical, diverse, and complex threat to national interests around the globe.

By defining information warfare as having two separate and distinct subsets, several assumptions are made about the subset relationship and how they interact. First, conflict is becoming more closely connected to the distribution of information. Cyberwar and netwar are modes of conflict that largely concern who knows what, when, where, and why, and how secure a society, military, or other actor is regarding its knowledge of itself and its opponents.[22] Second, a knowledge-based institution favors and strengthens non-hierarchical forms of organization, implying that relative advantage in the future will shift to networked opponents.

Networked forms of organization pose a significant threat for several reasons. If military theorists are correct in their predictions that future war is more likely to be diffuse, nonlinear, and multidimensional, then networked threats become more responsive to changing conditions on the battlefield. More importantly, networked threats pose significant problems to societies that possess high ethical and legal standards. Issues associated with complex humanitarian emergencies and terrorism consistently pose ethical and legal dilemmas for U.S. political and military leaders.

Networked organizations also have the capability to develop operational doctrine and strategies that are difficult to counter because of the force mix. Events in Somalia illustrated how

[21] Ibid.
[22] Ibid., 4.

problematic a mission becomes when networked threats use a combination of high-tech communications and low-tech strategies. Highly adaptable, networked threats thrive on dispersed operations using off-the-shelf technologies and decentralized command and control.

An archetypal netwar actor consists of a web (or network) of dispersed, interconnected "nodes" (or activity centers) – this is its key defining characteristic.[23] Each node may be built around a single entity, group, or fragments of groups in a formal or informal manner. There are no clear boundaries to a network and it may be loosely organized based on similar ideologies or interests. The organizational design parameters may be "all-channel," connected along a linear line of communication, or a central hub with supporting branches.

"All channel" networks are particularly difficult to counter because command and control nodes are not easily identified. Each node of the "all channel" network is designed to exist as a separate operating entity connected to all nodes within the network. Each node has the ability to work independently or together with other nodes given the specific nature of the mission. Whatever the organization looks like, it retains the ability to conduct like operations or divide and operate as highly specialized components.

The principle strength of the networked organization is embedded in the command and control structures, which are relatively flat. Netwar doctrine is built around the application of power without cumbersome hierarchical command structures. The most effective nets often operate with little or no leadership, relying instead on decision-making that is decentralized and based on consensus. Although networked organizations are often referred to as cell-based and identified with terrorist groups, the presence of cells does not always mean the network exists or is of an "all-channel" design.

The most effective networks normally have a nonhierarchical design tied to a powerful ideology or doctrine spanning the entire network. Networked organizations with embedded

[23] Ibid., 9.

ideologies and common objectives require little or no centralized command and control at the tactical level. Strategic and operational parameters set by ideology and doctrine establish direction for decision-making and execution at the lower levels.

However, the inherent weakness of the network design is a requirement for a well-developed communications infrastructure that transmits functional information. The informational requirements at the lower level are not always dependent on real-time communication, but when information is needed it is disseminated quickly and accurately throughout the organization. Unlike U.S. military organizations where command and control has become a function of how much information the commander needs and whether it is perfect information, networked threats do not depend heavily on situational awareness. What makes networks effective is their situational understanding.

CHAPTER 2

Netwar and Threat Adaptation

U.S. military strategists often approach the problem of developing a comprehensive defense strategy by looking at traditional threat-based templates from the Cold War. The current national security strategy notwithstanding, the focus remains force-oriented without any real consideration about how opponents will adapt to the application of technology-driven weapon systems. The dangerous assumption is that the environment of conflict has changed little in the past decade. Many military experts consider the strategy and doctrine used by Coalition forces in 1991 to defeat Iraq valid for the next century.

Yet as with any conflict, there are lessons learned on both sides. In his study of future war, Major General Robert Scales, Jr., concludes the following vulnerabilities for U.S. and allied forces exist.[24]

- U.S. aversion to casualties and excessive collateral damage
- Sensitivities to domestic and world opinion
- Lack of commitment to fight long wars or participate in military actions with no clear end-state
- Preoccupation with precision strike technology and digitized command and control

Potential threats that face U.S. applications of military force recognize that swift success is not essential to victory. Patience, when combined with will and the inherent power of the defense, can erode U.S. and allied resolve to remain engaged.[25] By distributing assets such as telecommunications, logistics, and transportation infrastructures in the field, the threat can limit the damage and duration of precision strikes.[26]

Threat adaptation is an evolving process over time and requires a deep understanding of the strategic environment at all levels. The underlying problem to faulty threat recognition is poor

[24] MG Scales, Jr., 48-49.
[25] Ibid.
[26] Ibid.

analysis. Threat organizations today are more elusive because they recognize that U.S. and allied forces possess a qualitative advantage in training, doctrine, and firepower. Most threats are developing strategies to bypass western military power in favor of attacks on peripheral targets that have second and third order effects on military organizations.

Threat organizations also recognize that U.S. and allied forces are force-projection oriented and therefore vulnerable prior to deployment. Operational threat strategies may take the form of asymmetrical attacks against supporting structures critical to force deployment and sustainment. Targeting to prevent entry to the region and the interdiction of air and sea points of departure could have lasting effects on the ability of the commander to accomplish the mission.

What troubles U.S. and other western military organizations are vulnerabilities that are intangible and difficult to measure. Examples include doctrine, the psychological will to fight, leadership decision cycles, public support for military operations, and relationships between coalitions. For the U.S., the issue of unacceptable casualty rates by the American public in operations without clearly defined end-states is problematic and commanders have been accused in the past of subordinating mission accomplishment to protection of the force.

Recognizing that the U.S. is without a military peer competitor, threat organizations seek to counter U.S. military dominance by creating conditions for stalemate. Attack is therefore, most likely to occur along a strategic axis with the goal of creating conditions for the strategic paralysis of the political decision-making process and operational paralysis of forces in the field. Recent operations in Kosovo, Somalia, Haiti, and Bosnia already indicate that uncertainty and problems with ethnic, cultural, and humanitarian issues complicate the decision-making process. Often the desire to see the issue through to the end dissolves because of the loss of public support, the impact of negative media content, and distributed threat psychological and deception operations that attack informational nodes, indirectly affecting command and control infrastructure. The threat understands that U.S. forces exist as a “system of systems” and that attacking the system enablers rather that the maneuver force is the best chance for success.

"Networked" organizations provide the greatest promise for less capable opponents to counter western military dominance. Using Arquilla and Ronfeldt's netwar model, the threat template changes dramatically. Assessing threat capabilities no longer becomes simply an exercise of locating the bulk of their forces and understanding their warfighting doctrine, but must also include an analysis of the political, economic, and societal organizations that influence how threat organizations fight.

New technologies make possible a "pure" variety of netwar in which all strategy and tactics – for example, disinformation campaigns and disruptive computer hacking – occur on "the internet" and in the media, but netwar also involves older technologies readily available at low cost to less developed states and non-state actors.[27] Though interaction among threat organizations is still driven by requirements for face-to face meetings, human couriers, and regular mail service, what has changed is the impact of technologies that allow less sophisticated opponents to coordinate, collect intelligence, and broadcast messages to target audiences.[28]

The move by states and non-state organizations away from direct confrontation with technologically superior military powers to network forms of warfare leverages the ability of transitional organizations not conforming to accepted norms of western-style democracy to achieve objectives based on their own terms. Because of globalization and the recognition that political, economic, and social institutions are more closely linked, opponents using netwar strategies have the ability to disrupt military forces by attacking non-military targets that impact on the decision making process.

Threat organizations also engage in similar planning cycles, identifying the "centers of gravity" and "decisive points" of the West, and developing strategies that focus on isolating

[27] John Arquilla and David Ronfeldt, "The Advent of Netwar," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt, (Santa Monica CA: RAND, 1997), 285.
[28] Ibid.

critical nodes that will cause systemic collapse when disabled or destroyed.[29] In most cases, because of the open nature of democratic governments and the impact of visual and print media on public opinion, ideal threat targets for "soft kill" or "non-lethal force" are the political leadership, belief systems, and economic infrastructures. Transportation and power grids also become key targets for computer generated attacks intended to paralyze command and control systems.

The real danger of netwar threat strategy is the network's ability to rapidly form and dissolve. It is possible that a threat network may organize as a kind of hybrid system when one node, such as a nation-state or governing organizations within a nation-sate, is connected to nodes that are transnational in nature with common strategic interests. The nation-state then may use transnational actors such as organized crime, non-governmental organizations, terrorists, or even contracted individuals to conduct discrete attacks against decision-making apparatus employing information technology, psychological warfare, or physical destruction.

Identifying its structure and then responding to how it executes operations makes the network difficult to counter. Networks are now defined more by "belief systems" than geographic boundaries and information technology allows them to organize rapidly, effectively, and dynamically. Consequently, targeting lines of communication and locating threat networks becomes difficult. To defeat threat networks, western militaries will have to mimic their operational capabilities, attacking networked organizations through networks.

Ironically, because the U.S. and the West depend heavily on the commercial sector to develop lead technologies, much of the latest technology is available off-the-shelf to potential opponents.

> Western information technology may well provide non-Western threats solutions to two significant problems. First, cellular technology and the internet may allow them to remain engaged

[29] John H. Miller, *Information Warfare: Issues and Perspectives* [database online] (Washington, DC: National Defense University, 1995, accessed 15 August 2000); available from http://www.ndu.edu/inss/siws/ch7.html.

> for long periods of time and maintain widely dispersed units. Second, the same technologies will allow them to rapidly mass when the opportunity arises for transition to the offense. Moreover, threat organizations are not hindered by the developmental costs associated with the acquisition of high technologies.[30]

This supports the notion that threat strategy for the next century will focus more on the disruption of institutions and military forces. The intent is to create stalemate and cause enough Western military casualties to pressure political leadership to opt-out of long term engagement, specifically in regional conflicts and intrastate war where U.S. and allied national interests and strategic objectives are not well defined.

One particular benefit of the information age for networked threats is the explosive growth of the internet and visual media technologies over the past decade. Both technologies provide a medium for conducting psychological warfare. China already recognizes the significant contribution of conducting psyop operations against an opponent.

> The current emphasis is on peacetime psychological operations. These operations set the stage for using information warfare during times of conflict. Technological developments have made it possible to subject all people, from commoner to heads of state, to a complex information offensive. Information media, such as language, texts, images and sound, as future weapons, exert a "multilevel operational effect" instead of simply a political or economic one. The target remains the enemy's decision-making process, both human (the mind) and material (hardware data processing).[31]

The media conduits available to threat organizations provide opportunities for the conduct of psychological warfare against military and civilian organizations.

In a broader sense, the media is benefiting from the same technology that gives the U.S. and allied militaries their edge. They are far more independent and skeptical in their coverage of military actions and the political gamesmanship that precipitates the application of force. The

[30] MG Scales, Jr., 52.
[31] LTC Timothy L. Thomas, USA (Ret.) *Military and C4I* [database online] (Infowar.com, Ltd., 3/21/00, accessed 05 August 2000); available from http://www.infowar.com/mil_c4i/00/mil_c4I_032100a_j.shtml.

media now provides viewers, listeners, and readers almost instant access to the battlefield, no matter how remote, with computers, cell phones, and satellite up-links.[32] Manipulated effectively by networked threat organizations, the media may become an unknowing participant in a strategy designed to disrupt the decision-making cycle by eroding public support through disinformation campaigns.

Today control of information from media outlets is almost impossible due to the number of outlets and the open access to internet technologies. In a strategic campaign, the line between information warfare waged against the threat and the information warfare waged against the U.S. and her allies is easily blurred.[33] Because the media have access to threats as well as friendly forces, the execution of strategic information warfare may involve the deception of the media as well. The development is a disturbing one since a netwar strategy might involve feeding the media continuous images and stories that erode public confidence in continuing military operations.

Perception management as a tool is essential and the use of deception is a fundamental tenet of war.[34] The target of deception is the decision-making process, to alter the beliefs of the people who support the appointed leadership responsible for directing the execution of diplomatic and military missions.[35] Colonel Richard Szafranski, stated the concept theoretically, "An aim of warfare has always been to affect the enemy's information systems." His considerations for attacking include "every means by which and adversary arrives at knowledge or beliefs" in that context.[36] Applied to threat strategy that targets western opponents, the intent clearly becomes

---

[32] Douglas Waller, "Public Affairs, Media, and War in the Information Age," in *War in the Information Age: New Challenges for U.S. Security Policy*, ed. Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., (Washington: Brassey's, 1997), 322-324.
[33] Ibid., 329.
[34] John B. Alexander, *Future War: Non-Lethal Weapons in Twenty-First-Century Warfare*, New York: St. Matin's Press, 1999), 111.
[35] Ibid.
[36] Colonel Richard Szafranski, quoted in John B. Alexander, *Future War: Non-Lethal Weapons in Twenty-First-Century Warfare*, New York: St. Matin's Press, 1999), 111.

one of directing information attacks designed to undermine or disrupt the functions of organizations that depend on the collection of accurate and factual intelligence about the enemy.

What advantages do threat networks possess when considering organization and the availability of information and technology? If the notion is correct that threat organizations have the capability to organize and dissipate rapidly, then the ability to paralyze hierarchical institutions such as the political and military organizations of the U.S. and her allies is evident. Threat adaptation is focused toward building decentralized networks (either state-centric, non-state centric, or a hybrid of both) that attack the decision-making processes. Western institutions become vulnerable through information overload. By flooding the information network, specifically nodes that focus on the collection of intelligence and the transfer of information to the masses, a form of "analysis paralysis" (indecision resulting from forever waiting for the next piece of information) occurs.[37]

Since information warfare transcends traditional modes of conflict, the potential to achieve conflict resolution in favor of the enemy increases significantly. Disrupting the flow of data to well-developed nations with integrated economic systems sensitive to uncertainty and instability might lead to panic if actors perceive that wealth-creating institutions are at risk. The arrest and prosecution of Vladimir Levin and Kevin Mitnick illustrates the impact of being able to illegally access (hack) secure computer systems. Albeit each acted alone, the intrusions caused millions of dollars in damage and resulted in millions of dollars of software being stolen.[38] Threats of this type, or more accurately individuals with information warfare capabilities that are integrated with less sophisticated networked organizations, have the potential to disrupt information flows that are critical to the sustainment of high-tech industries and financial

[37] John Arquilla and David Ronfeldt, review of *In Athena's Camp: Preparing for Conflict in the Information Age,* by Brent Stuart Goodwin, *Naval War College Review* (Spring 2000).

[38] Alexander, 109.

institutions dependent on information. Any disruption to the flow of critical information sets in motion the potential for collapse.

CHAPTER 3

Threat Adaptation: Case History

Students of military theory and doctrine have focused on the impact of information technology on the operational capabilities of U.S. and allied forces for much of the last decade. A significant amount of literature has been devoted to explaining the ongoing "revolution in military affairs" and the implications of modern warfighting in the future. Yet, only recently has there been any attempt to understand how organizations that pose a threat to the security of the Western world will adapt to the presence of U.S. military dominance.

The best illustrations for understanding how the threat is adapting to U.S. and allied military superiority are contained in the recent case history of operations since the conclusion of Desert Storm. For the purpose of this study, three case histories have been selected for analysis: U.S. involvement in Somalia, the U.S. air campaign in Kosovo, and the Zapatista rebellion in Mexico. Each case history is unique in it's own right, and illustrates how threat states and non-states may organize against Western intervention in the future. Except for the Zapatista movement in Mexico, the case histories show that intervention and the subsequent application of military power by the U.S. and her allies became an outgrowth of a failed diplomatic policy attempting to resolve a complex humanitarian emergency.

Though sufficient evidence is lacking on how threats adapt when confronted by high-intensity conflict, the three case studies are relevant to future threat adaptation based on the characteristics and behavior by threat structures unique to each conflict. Analysis of the three case histories seems to confirm that future threats may adapt by seeking stalemate through the disruption of public support and political, military command and control nodes. Each case contains a threat dimension that used a form of netwar against the opponent, and each case indicates an operational threat strategy based on the use of information warfare and networked organizations that may be the harbinger of expanding threat operations in the future.

Somalia

The events in Somalia leading to the total withdrawal of United States and United Nations military forces are benchmarks for a humanitarian peacekeeping operation gone bad. Intervention by the West was precipitated by the media's unrelenting focus on a situation where civil unrest had descended into total anarchy with the collapse of Somali President Siad Barre's regime in 1991. What prompted the intervention initially was the desire to mitigate the immeasurable human suffering caused by clan warfare and widespread famine.

The roots of the Somali conflict are imbedded in a military coup that brought Siad Barre to power in 1969, claiming not only the institution of a new political order but also proposing the radical transformation of Somali society through the application of "scientific socialism."[39] Though Somalia is frequently described as a "failed state," it has existed primarily in name only with little or no central government, instead ruled through a complex and diverse clan system corrupted by centuries of colonialism and Cold War geopolitics.[40]

Somali politics presented unique problems for western peacekeepers sent to relieve the ongoing suffering and starvation of its people. Historically, the Somali clan system does not formally recognize the role of a single authoritative hierarchical entity. The traditional well-defined political and economic institutions common to western nation-state systems never existed. Rather the mechanisms for conflict resolution resided within tribal clans, predominately organized along lines of paternal kinship. The lineages prevented escalation by inhibiting economic stratification, which later became refined and governed by Islamic law.[41]

The basis for organization of Somali society rested on six dominant clan families. Each clan family was further subdivided into sub-clans and lineages which continually created and

---

[39] Robert Kaplan et al. *Somalia Area Handbook* [database online] (Washington, DC: U.S. Government Printing Office, SO0002 – SO0131, accessed 03 August 2000); available from http://lcweb2.loc.gov/c…cs:@field/DOCID+so0002.
[40] Thomas G. Weiss, *Military-Civilian Interactions: Intervening in Humanitarian Crisis* (New York: Rowman & Littlefield, Inc., 1999), 71.
[41] Ibid., 71-72.

shifted alliances among themselves, an inherent complexity of tribal society.[42] The understanding of how the clan systems were interconnected and functioned was necessary to dealing with what was perceived to be a state of anarchy.

The impact of clan infighting and the absence of any legitimate controlling government in Somalia alerted the attention of the U.S. and the rest of the world. American embassy workers had already been evacuated, but worsening conditions accentuated by the media and reports from non-governmental organizations (NGO) continued to have an impact and prompted U.S. policy makers to approve a military airlift of food and medicine to the beleaguered nation.[43] The crisis had remained largely beyond the purview of the international community until 1992, when disturbing images of massed starvation, lawlessness, and the diversion of critical relief supplies by armed banditry caused increased pressure in the West for more effective action to stabilize the conflict.[44]

The ensuing operations co-sponsored by the U.S. and the United Nations (UNOSOM I and II) met with little success in achieving the goal of restoring a viable government and alleviating the deteriorating social conditions. Both U.N. operations were politically weak and pursued ad-hoc policies. The more powerful and larger U.S. led Unified Task Force (UNITAF) had the resources but insisted that its mandate was nonpolitical and limited to humanitarian relief operations.[45]

Complicating matters was the presence of a number of organizations in country for humanitarian purposes with divergent and conflicting agendas. The Somali clan leadership recognized that the weakness of the humanitarian effort offered an opportunity for exploitation

[42] Ibid., 72.
[43] John G. Fox, "Approaching Humanitarian Intervention Strategically: The Case of Somalia," in *Essays 2000: Chairman of the Joint Chiefs of Staff Strategy Essay Competition*, ed. General Henry K. Shelton, (Washington, DC: National Defense University Press, 2000), 36-38.
[44] Terrance Lyons and Ahmed I. Samatar, *Somalia: State Collapse, Multilateral Intervention and Strategies for Political Reconstruction* (Washington, DC: The Brookings Institution, 1995), 31.
[45] Ibid., 36.

and consciously pursued diverse strategies as conditions changed to ensure the maintenance of a power base among local populations within clan boundaries.[46]

Despite the U.S. desire to stay focused on the Somali disaster as a purely humanitarian operation, the presence of a large military security force changed the political landscape, inviting escalation.[47] UNITAF was soon directed to embark on a nation building exercise coupled with the application of military force to eradicate or co-op clan leadership. Already operating under a restrictive peacekeeping security mandate, UNITAF failed to recognize that, to effect a transition from a state of anarchy, a coalition among Somali clans would be required to file the political vacuum.[48]

The ensuing military debacle on October 3, 1993 ultimately resulted in the complete withdrawal of UNITAF and UNISOM missions after the death of 18 U.S. Army Rangers and hundreds of Somali civilians and clan militia fighters. The misguided U.S. policy of attempting to capture a prominent clan leader, Mohammed Aideed, for his authorizing indiscriminate attacks against U.N. and U.S. peacekeepers, backfired and destroyed any hope for reconciliation among the clan factions and any support for transition to a legitimate, functioning government.

The Somali disaster serves as a benchmark for the study of how the threat is adapting to the application of conventional military force to military operations other than war (MOOTW). Somali clans understood early on that the use of U.S. military force was limited by the rules of engagement and that the escalation of conflict with peacekeeping forces would act as a combat multiplier for the Somali militia. The inherent makeup of Somali society and the existing links between clans illustrates how a low-tech adversary takes advantage of a network to offset U.S. and U.N qualitative advantages in men and materiel.

Despite ongoing disputes among clan leaders over territory and access to resources, the

[46] Ibid., 36-37.
[47] Walter S. Clarke, "Testing the World's Resolve in Somalia," *Parameters,* vol. 23 (Winter 1993-94), 42.
[48] Terrance Lyons and Ahmed I. Samatar, 37.

operational environment was defined by the clan's ability to act as a coalition to counter the increase in the use of U.S. military force. Clan leaders and their followers were united by a common cause, to preserve the clan way of life, which happened to be directly linked to lessening the influence of U.S. military forces within their regions.

Three distinct trends emerged that indicate Somali militias were adapting new operational strategy to the presence of overwhelming U.S. military superiority. First, the role of the media and the images portrayed throughout the conflict had a significant impact on American foreign policy. Initially the West had ignored the suffering and viewed the situation as nothing but another civil war among tribal societies in Africa. However, the NGOs working in the region began to put pressure on governments to provide assistance through numerous media outlets. Major international organizations, such as the International Committee of the Red Cross and the U.S.-based CARE, lobbied aggressively for international involvement.[49] By the time serious consideration for U.S. intervention had been discussed by the Bush administration, editorials with titles like "The Hell Called Somalia" had appeared nationally along with a parade of prominent American individuals and celebrities speaking out in support of a humanitarian mission.[50]

Once the U.S. intervened and the mission gradually changed from one of humanitarian peacekeeping to one of peace enforcement, the images of violence had a very different effect. Within hours of the combat action in which 18 Americans died, CNN and other major news networks brought home to the American public the inherent dangers of peacekeeping and humanitarian missions. The pictures generated of an American helicopter pilot's body being dragged through the streets of Mogadishu and the TV appearance of a bloodied and bruised

[49] Ibid., 31-32.
[50] Ibid.

Michael Durant, another pilot being held hostage, immediately brought into question the presence of UNITAF in Somalia.[51]

The incident involving the combat deaths of the Army Rangers and the shootdown of two American helicopters set in motion the erosion of public support for what was assumed to be a peaceful operation. Within days, Congress and the White House assessed that the public would no longer support the deployment and made plans for withdrawal. On a much larger scale, the media reporting of the incident and the subsequent public reaction caused the Clinton administration to be more cautious about committing to future peacekeeping and humanitarian missions and less likely to risk American casualties.[52]

The second trend is that despite advanced weapons systems and information technology; low-tech adversaries have an innate ability to avoid detection by hiding within their clan networks. The clan militia engaged U.S. and U.N. forces only when it was to clan advantage, and in the case of the events leading to U.S. withdrawal, clan networks demonstrated that Somali intelligence was effective in disseminating information about U.S. troop movements and tactics. Much of the information was transferred throughout the Somali network using cell phone technology and one-on-one contact with operatives working in U.S. and U.N. compounds.[53]

The third trend suggests that decision-making cycles are vulnerable to the spinning of information. The media impact and the erosion of public support after the death of American soldiers validates the notion that how information is received and processed significantly impacts on the decision-making process. Threat networks that can affect the collection and distribution of information have a distinct advantage if the information being processed disrupts the interaction between decision-makers. Because most Western societies govern by consensus among elected

---

[51] James Adams, "The Role of the Media," in *Cyberwar: Security, Strategy, and Conflict in the Information Age,* ed. Alan D. Campen, Douglas H. Dearth, R. Thomas Gooden, (Fairfax, VA: AFCEA International Press, 1996), 110-111.
[52] Fox, 35.
[53] James Adams, *The Next World War: Computers are the Weapons and the Front Line is Everywhere* (New York: Simon & Schuster, 1998), 60-75.

representatives, networks that attack the decision cycle with disinformation or manipulated information realize success when the policy-making process becomes bogged down by indecision, or when consensus among the key players becomes fractured. In the case of Somalia, the conduct of the mission, the mission's effect on the political-military situation in Somalia and, later, the tension with the U.N. over the conduct of the operation, as well as by the interagency process, influenced the decision to continue humanitarian and peace enforcement operations.[54]

In summary, the failure and subsequent withdrawal from the Somali peacekeeping and humanitarian mission set the stage for future debate over the role of American peacekeeping forces. More importantly, opponents of the U.S. and her allies took away valuable lessons that would later be refined into an ad-hoc threat doctrine. Somalia became a victory not only for Somali clans, but also for state and non-state threats looking for alternative strategies to counter the application of U.S. military force to stabilize regional conflict.

Kosovo

The analysis of NATO's military action in Kosovo offers unique insight into adaptive threat strategies. The genesis of the conflict is rooted in ethnic and cultural tensions that have been pervasive throughout the Balkan region since the collapse of the Ottoman Empire. The problem that remains the central focus of the post-Cold War era is the synthesis of east-west conflict over independence and state formation that was also the source of conflict for much of the nineteenth and early twentieth centuries.

The dynamics of today's conflict are rooted in President Slobodan Milosevic's ideology of Greater Serbia, born out of the collapse of Yugoslavian Marxism and conforming to the classic patterns of east-west conflict.[55] It is the east-west intersection that has formed the strategic context of conflict within the Balkan region for much of the past decade. The Balkan situation

[54] Fox, 36.

promoted completion of the NATO transformation from a European defense alliance to a security alliance capable of responding to regional crises that threaten stability.

Violence again erupted in the region in March 1998, and for the third time in a decade the root cause was embedded in the nationalist politics of President Milosevic. His stated intent was to reclaim land that was of cultural, historical, and religious importance for the establishment of a Greater Serbia. Once Milosevic began his ethnic-cleansing program to rid the region of Kosovar Albanians, images of the brutal and systematic extermination of the local population mobilized the United States and its European Allies to seek a political solution to avoid further escalation of an intrastate conflict that could threaten European stability.[56]

Past humanitarian disasters in the Balkans left hundreds of thousands of Bosniacs, Croats, and Serbs dead and millions displaced. Now the same type of catastrophe seemed likely in Kosovo and threatened to spill over into the neighboring states of Albania and Macedonia, which would affect the stability of the entire Mediterranean basin.

For more than a year, the civil war had festered between the Kosovo Liberation Army (KLA), local Albanian supporters of the KLA, and Serbian security forces. Repeated attempts by the United States and NATO to find a diplomatic settlement with Serbia failed, and Milosevic displayed little interest in reaching a negotiated settlement with an alliance that he assumed would never reach a consensus about how and to what extent they would prosecute a war.[57] Consequently, NATO began a limited bombing campaign against Serbian forces hoping that Milosevic would return to the negotiating table. NATO's strategic goal was find a way short of independence to protect ethnic Albanians and force the removal of all Serbia military forces from the Kosovo province.[58]

---

[55] Michael Evans, *Dark Victory: The Use of Military Force in Kosovo*, Working Paper No. 54 (Canberra Australia: Australian Defense Force Academy, 1999).
[56] Ivo H. Daalder and Michael E. O'Hanlon, *Winning Ugly: NATO's War to Save Kosovo* (Washington, DC: Brookings Institution Press, 2000), vii.
[57] Ibid., 1.
[58] Ibid.

NATO initially expected the bombing campaign to last only seven or eight days. However, political advisors and military planners underestimated the resolve of President Milosevic and the Serbian people and the air campaign stretched into a seventy-eight day operation.

> Despite the presence of overwhelming military power, the early phases of the conflict were dominated by Serb actions in Kosovo. Up to 10,000 Kosovars died at Serb hands; thousands more were raped or otherwise brutalized, and some 800,000 more forcefully expelled from the province. Ultimately perhaps 1,000 to 2,000 Serbs perished; to include civilians killed by collateral damage and Serb forces on the battlefield.[59]

After almost three months of non-stop bombing, Serbia culminated and Milosevic returned to the bargaining table. NATO considered the operation a significant victory and demonstrated that judicious use of military force was an effective instrument for conflict resolution.

Yet, the continuing debate among policy analysts is how effective was NATO's bombing campaign in achieving the desired results. Perhaps a more relevant question is whether Serbia used adaptive strategies to counter the presence of superior conventional military power and whether they achieved the goal of creating a stalemate, albeit for a limited period of time. The Serb reaction to NATO precision strikes mirrored that of the Vietnamese a quarter of a century earlier, that of dispersion and deception. Without the presence of a ground threat on their border, Serb forces felt relatively secure remaining hidden and virtually immune to high-altitude bombing.[60] Like the Somalis, Serbian military forces demonstrated that they were a learning organization and capable of adapting to the new realities of post-Cold War warfare.

Unlike the Somalia experience, the United States was not conducting military operations against a third-rate non-state entity. Serbia possessed advanced weaponry of Soviet design and a

---

[59] Ibid., 3.

[60] MG Robert H. Scales, Jr., "From Korea to Kosovo: America's Army Learns to Fight Limited Wars in the Age of Precision Strikes," *Armed Forces Journal International* [database online] (December 1999, accessed 06 September 2000); available from http://www.afji.com/mags/1999/december/fromkoreatokosovo/index.html.
.

robust information infrastructure that supported non-military targeting. What made the war in Kosovo unique was the opportunity to measure the impact of the information revolution on traditional military organizations.

Analysis of events in Kosovo indicate that the Serbian response to the threat of the use of Allied military force to compel Milosevic to negotiate triggered defensive and offensive reactions that support Arquilla and Rondfelt's netwar theory. Historically, the Serbian President consolidated his power through what Michael Ignatieff calls "a new style of post-Cold War authoritarian populism." Explaining further, Ignatieff posits that Milosevic was "neither a Pinochet, dependent on tanks, nor a Ceaucescu, dependent on the security police," rather he was the arbiter of a collection of factions that intensely distrusted and disliked each other.[61]

The value of Ignatieff's assessment is inherent in the presence of a form of networked organization with a certain degree of resilience to NATO pressure to cease the extermination of ethnic Albanians. Milosevic's strength was his coalition, not his military forces. As long as he maintained a base of popular support, he was insulated from western diplomatic coercion.

The Milosevic regime exhibited characteristics of a state-centric threat organization with the capability to possibly exploit Western vulnerabilities. Clearly he understood the potential for the use of media images and information broadcasts to undermine support for NATO and the U.S. and to solidify his own support at home. By allowing CNN and the BBC continued access to media outlets from within Serbia, Milosevic hoped to destabilize Western opinion with images and stories of civilians killed by NATO's indiscriminate bombing.[62] Milosevic had learned his lessons well from Saddam Hussein about manipulation of the information spectrum.

Although the air war over Serbia was the main focus, both sides also waged a media war. Nightly broadcasts that addressed Allied progress and the attempt to accurately measure battle damage were turned into messages that NATO was defending the defenseless, yet Milosevic

[61] Michael Ignatieff, *Virtual War: Kosovo and Beyond* (New York: Metropolitan Books, 2000), 51.
[62] Ibid., 52.

turned the same information against NATO by claiming that allied bombing was intentionally targeting the defenseless Serbian peoples.[63] For the most part, NATO was unprepared for the information war waged by Milosevic.

Another benefit to Milosevic of waging an information war was linked to buying time to continue the systematic extermination of ethnic Albanians in Kosovo. In fact, indicators suggest that the Serbian army, police, and paramilitary units murdered as many as 10,000 Kosovar Albanians during the execution of Operation Allied Force.[64] Because force protection issues ruled out the use of ground troops from the operation and caused airstrikes to be restricted to high-altitudes, Serbian forces operated during hours of limited visibility with relative freedom to continue dispersed ethnic cleansing operations throughout the province.

A more disturbing trend is a continued focus on casualty aversion by U.S. political and military leadership. Major General Robert Scales, Jr. best articulates the preoccupation with casualty aversion.

> Casualties soon may represent a dominant, perhaps the dominant measure of success or failure in wars of limited ends and means such as Operation Allied Force in Kosovo. Dead Americans are becoming our most vulnerable center of gravity – and our enemies know it. As we saw in Kosovo, serious doubts on the part of our national leaders about casualties may not only delay, but may well prevent commitment of ground forces.[65]

The key point that MG Scales makes is that casualty aversion has become a strategic center of gravity and that force protection issues before consideration of strategic and operational objectives drive decisions on the use of force in the future.

To summarize, Operation Allied Force exposed some fundamental truths about how the enemy is adapting to U.S. and Allied force projection and technological superiority. Many argue

---

[63] James O. Kitfield, "Command and Control: The Messenger," *National Journal* (September 11, 1999), 2546.
[64] Alan Stephens, *Kosovo or the Future of War*, Working Paper No. 54 (Canberra Australia: Australian Defense Force Academy, 1999). 1-22.
[65] MG Scales, "From Korea to Kosovo: America's Army Learns to Fight Limited Wars in the Age of Precision Strikes."

that the potential number of casualties associated with ground operations prohibited the early entry of ground forces to flush Serbian targets for precision strikes. The second and third order effects of not using ground forces during the campaign contributed to Milosevic's gamble to continue ethnic cleansing of the Kosovar Albanian population.

Secondly, the use of information operations by both sides to enhance perception management of the war became a test of wills. In a broader context, the information war became a non-lethal tool to disrupt the decision-cycle of both the Serbian and Allied leadership. NATO eventually won out, but not without consequences for the long-term. Conflict between Lieutenant General Michael Short, the air component commander, and General Wesley Clark, the NATO commander, over targeting issues may have set a precedent for future conflict between commanders with differing opinions about how to attack enemy centers of gravity. Although considered a minor problem, the conflict between Lt. Gen. Short and Gen. Clark indicates that vulnerabilities do exist in U.S. command and control relationships.

Milosevic continually adapted to changing conditions with the intent of paralyzing the strategic and operational decision making process. Although somewhat effective against targets within NATO, information campaigns directed at undermining public support for the operation in the U.S. had limited effect. Yet, indicators suggest that if the campaign had stretched beyond ninety days, the negative effects on public support might have materialized despite NATO's attention to conditioning world opinion by a measured and steady increase in the use of airpower, which minimized casualties.[66]

Finally, in spite of NATO's near total information superiority, Serbian forces consistently manipulated NATO's battlespace awareness through the use of deception and hide-and-seek tactics.[67] The exploitation by Serbian forces of NATO's strict rules of engagement allowed for the

[66] Stephens, 14.
[67] Timothy L. Thomas, "Kosovo and the Current Myth of Information Superiority," *Parameters* [database online] (Spring 2000, accessed 15 September 2000), available at http://carlisle-www.army.mil/usawc/parameters/00spring/thomas.htm.

movement of equipment to avoid detection and the construction of decoys that skewed NATO's battle damage assessment figures. At the end of the air war, hundreds of destroyed Serbian targets were later discounted as decoys. NATO's collection assets and interpreters were fooled by Serbian offsets that included deception, disinformation, camouflage, the clever use of radar, spies within NATO, undetected helicopter movements, and the exploitation of NATO's operational templating of information-dominance activities.[68]

In retrospect, Milosevic's success at countering Allied combat operations suggests that future threats are improving their ability to develop adaptive operational strategies designed to attack high technology systems by creating sensory overload or the denial of information to collection assets. Serbian information campaigns demonstrated that networked organizations using cyberwar techniques have the potential to disrupt friendly decision-cycles, ultimately creating greater friction within the spectrum of conflict and either buying time or creating conditions for stalemate.

Zapatista Netwar

The strategies used by the Zapatista National Liberation Army (EZLN) illustrate the dynamic potential for the use of netwar against opponents possessing superior political and military power. On New Year's Day, 1994, two to four thousand insurgents of the EZLN occupied six towns in Chiapas, Mexico, demanding social, economic, and political reform of the incumbent Mexican government.[69] The Mexican government responded in a traditional way by deploying a significant number of military and security forces to the Chiapas region. Government officials simply viewed the insurrection as limited in scope and confined to the region.

[68] Ibid.
[69] David Ronfeldt and Armando Martinez, "A Comment on the Zapatista Netwar," in *Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt, (Santa Monica CA: RAND, 1997), 369.

Yet, what made the Zapatista insurrection unique were the methods by which the EZLN broadcasted its message. Utilizing various media outlets and connections with international organizations the Zapatista's called on civil society to engage in a nation-wide struggle to reform social, economic, and political institutions without taking up arms.[70] The EZLN intent was not to seize power or to implement a new ideology, but designed to mobilize national support for a true democracy based on a legitimate government and fair elections. Additionally, they requested that international organizations (notably, the Red Cross) and civil-society actors (human-rights groups) from around the world monitor the conflict and validate the notion that the uprising was not tied to Marxist or other standard ideologies, but was instead indigenous by nature.[71]

The rapid response by the Mexican government with military force against rebel-held strongholds and the reports of human-rights abuses fueled further interest by outside actors. As the EZLN gradually withdrew from the towns to the safety of the Chiapas jungles, representatives from human-rights groups and non-governmental organizations (NGOs) converged on Mexico City and Chiapas in support of the Zapatista cause. The ensuing international "swarm" (electronically as well as physically) put immense pressure on the Mexican government to seek a non-violent resolution to the conflict and to allow journalists and NGOs to monitor conditions in the affected regions.[72]

Unlike insurgencies of the past, the "social netwar" waged by the Zapatista's was directly linked to the ability of the EZLN and NGOs to form highly networked, transnational coalitions capable of exploiting information-age technologies to enlist international and indigenous support for EZLN objectives. The links to transnational and local NGOs that claim to represent civil society allowed the movement to evolve from a classic "insurgency" framework to an

[70] Ibid., 370.
[71] Ibid.
[72] For further discussion of the concept of swarm networks and how they work see Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World* (New York: Addison-Wesley Publishing Co., 1994), Chapter 2.

information age netwar framework.[73] Without the netwar framework, the EZLN insurgency would most likely have turned into a conventional counterinsurgency by the Mexican government.

Future study of the affects of the Zapatista netwar suggests that information and information-age technologies are altering the nature of conflict. The ability to use information operations to dominate the "information space" allowed the EZLN to leverage the power of NGOs, the media, and intellectuals to effectively paralyze the Mexican government. The potential for negative public perceptions by the international community forced two Mexican presidents to cease combat operations and seek a political settlement. At stake was the image of a destabilized Mexico, which could lead to the withdrawal of foreign investment critical to Mexican economic development.

Although the netwar between the EZLN and Mexico's government is far from over, the nature of the conflict demonstrates that networked organizations have the capacity to alter the balance of power between powerful state-centric organizations and less powerful non-state entities. Netwar confirms that hierarchies, such as the Mexican government and the Mexican army, do have difficulty in fighting networked organizations.[74] More importantly, the linkages between the FZLN and the NGOs demonstrate that transnational actors have the ability to act collectively when possessing similar ideological and political goals. In the Zapatista's case the shift in strategy away from direct military confrontation to "social netwar" created strategic and operational paralysis within Mexico's government and army.

[73] Ronfeldt and Martinez, 371.
[74] Ibid., 384.

CHAPTER 4

Conclusion

Threat entities are adapting to successfully deal with the projection of superior military power. Based on the case histories cited, it can be concluded that threats to the security of the United States and her allies might achieve the operational and strategic paralysis of U.S. and allied military forces through “netwar strategies.”

Several key assumptions about the new strategic environment must be articulated. First, the United States currently maintains status as the premier military power. No peer competitor exists or is likely to exist in the near future. Consequently, the U.S. capability to project power worldwide is a strength unmatched by any other developed nation-state. High technology is a hallmark of U.S. power projection, but brings with it significant vulnerabilities.

Second, despite our power projection capabilities and the envious position of being one of the wealthiest nations in the world, relationships among all states are weaker and more fluid due to the lack of a single monolithic threat. Third, the inherent drawback accompanying the transition from the industrial age to the information age is the perceived reduction of stability and predictability in the realm of domestic and international politics. Consequently, the potential for conflict internally and externally increases as more groups with similar interests seek autonomy or independence.

Fourth, because of globalization and the collapse of traditional Cold War structures, the potential for regional conflict is increasing. States that once were controlled by the Soviet Union have dissolved and are reorganizing along more ethnic and cultural lines. Persistent low-intensity conflict marked by intrastate warfare sets conditions for escalation to mid-intensity conflict which contributes to regional destabilization. The political complexity and intensity of intrastate warfare and the extensive impact of humanitarian disasters on civil society raise problems that defy the simple application of discriminate force as a tool for conflict resolution. The trend over the last

decade is the expansion of military operations other than war (MOOTW) and the increased use of the military as a first choice response when confronted with complex humanitarian emergencies.

Finally, the rise of transnational actors as key players in the international environment becomes problematic for traditional nation states. Information age technologies act as catalysts for non-state organizations that seek to exercise power at the same level as developed nation states. Technology creates opportunities for hybrid forms of transnational actors to impact upon the decision-making process of more powerful states, in some cases causing them to readjust foreign policy in favor of minority organizations with specific agendas or a common set of goals.

Despite trends that suggest the international environment is undergoing significant change, the nation-state remains a significant player in international relations. Developed states such as the United States with robust political, economic, military, and social institutions will continue to lead the rest of the world into the next century. However, the pace at which change is occurring reflects the impact of the information revolution.

Interdependence among states has always existed, but is becoming more complex because of the availability of information. The small cost of transmitting messages and transferring data in near real-time across the globe increasingly provides opportunities for multiple social and political relationships to be formed, endowing non-state actors with enormous amounts of “soft-power” that influence or even paralyze the ability of states to engage in controversial international activities.

The changing environment and the information revolution also provides opportunities for new threats to arise. The leveling effect of the information revolution reduces the barriers of entry to threat states and organizations. The distributed and nondescript nature of the world-wide-web allows states and non-state actors with agendas that threaten regional stability to become more difficult to counter and assign accountability. Many of them recognize that direct confrontation with more powerful states, specifically states that possess strong military organizations, is not desired and seek alternative methods of warfare.

The emphasis on studying the impact of the information revolution has produced numerous theories about how war will be fought in the future. The emphasis herein has been on Arquilla and Ronfeldt's model of "netwar" developed at the RAND Institute. Studying netwar offers insight into how threat organizations are adapting to the more frequent use of conventional military power to terminate conflict on threat terms but short of total war.

The precise definition of netwar refers to the emerging mode of conflict at societal levels where threat organizations use network forms of organization along with related doctrines, strategies, and information-age technologies to achieve goals and objectives. What makes netwar dangerous to conventional militaries and state structures is the ability it affords threat actors to communicate and coordinate their activities across all global boundaries using information-age technologies. Access to information about threat opponents is less restricted because of its availability through more open and diverse communication nodes such as CNN and the Internet.

Networked threats do not depend on hierarchical organizations, doctrine, and strategies to execute missions against nation-states projecting conventional military power. Because they are diffuse in nature and have flattened command and control structures, networked threats easily form and disperse as necessary. The real danger of networked organizations is their ability to build hybrid organizations that attack not only military targets, but also political, economic, and societal infrastructures. Hybrid organizations may take on the appearance of a state structure with limited conventional military means enhanced by smaller transnational actors (e.g. organized crime, NGOs, single issue militant organizations, terrorists) with the capability to conduct netwar simultaneously with limited combat operations. Any number of variants is possible with the intent to destroy or disrupt diplomatic and military missions, or both.

U.S. and allied intervention in Somalia and Kosovo provided insight into how threat organizations adapt to the changing conditions of warfare. Somalia clansmen and militia operated against the high-tech U.S. forces at very low levels of sophistication. Yet, the Somalis were able to take advantage understanding how U.S. military operations were conducted and the impact of

heavily restrictive rules of engagement. Somali militia also relied on off-the-shelf technology (e.g. cell phones, walkie-talkies) to enhance traditional methods of communication. Although Somali clan relationships were in a state of constant flux, they possessed the ability to form and disperse when needed as a network to engage U.S. and allied forces.

The significant impact of events in Somalia was the recognition of the media as a player in perception management. The real-time transmission of events and the impact generated on the American public by scenes of brutality against U.S. servicemen validates the notion that perception management has the potential to disrupt decision-making cycles. The outrage expressed by Americans over events in Somalia and the erosion of public support for U.S. policy illustrate the effectiveness of information war waged by a clever opponent. The eventual withdrawal of U.S. forces from Somalia signaled that domestic criticism and the erosion of public support could influence U.S. decision-making.

The NATO air campaign over Kosovo and the confrontation with Serbia's President Milosevic signaled once again the impact of perception management on coalition combat actions. Initially the focus had been on political and military issues surrounding the extermination of Kosovar Albanians and the subsequent response by the international community. Yet, early in the campaign a small number of Kosovars killed by Allied bombing touched off a media firestorm that focused on a single tactical event. The ensuing debate by the media with NATO over the mistaken targets exposed weaknesses in the alliance's command and control relationships, which were later brought to the front publicly by the report concerning Lieutenant General Short's disagreement with General Clark about targeting.

Although Milosevic's regime became a casualty of NATO airpower, the important lessons taken away from the conflict between Serbia and NATO are tied to how the threat adapted to the application of overwhelming military power. Milosevic sought to create a stalemate with NATO initially through diplomatic maneuver. However, once NATO resorted to

the use of force, Serbian strategy shifted to deception tactics, specifically by hiding air defense assets. The objective was to buy time to allow the completion of the ethnic cleansing of Kosovo.

Simultaneously, Milosevic waged and information war against the U.S. and NATO. It could be argued that the information campaign achieved limited success initially, but could not sustain itself due to the lack of supporting networks. However, Serbian information warfare reinforces the inherent value and power of public opinion. The campaign also exposed the problem of targeting elements of threat infrastructure that support the transfer of information. Physical destruction may not always be necessary, but it may have the potential to be detrimental to occupying forces since the future use of facilities may be critical to post-hostility operations.

The Zapatista insurrection has implications that extend beyond Mexico. Furthermore the linkages between the EZLN and transnational actors, establishes a prototypical model for the transformation of organizations that are significant threats to the U.S. and her allies. Examples include networked criminal organizations that continue to be a growing threat because of the ability to leverage global and regional connections. Although diverse in organization and ideology, they have the capability to operate freely across borders, remain mobile, and easily adapt to changing economic, political, and social conditions.

More importantly, organizations based on the Zapatista “social netwar” model create conditions where conventional peacekeeping and peace enforcement strategies do not always work. The failure to integrate influential NGOs networked with other civil-society actors that have robust organizational, technological, and social infrastructures into U.S. and allied military operations could significantly degrade operational capabilities.

The relevance of examining threat adaptation and the use of information warfare as an enabler is apparent. The information age is changing how combatants execute operations within the spectrum of conflict. The emphasis is on creating networked organizations with the influence to alter public opinion through the various forms of media. Additionally, building hybrid organizations capable of exploiting the strengths of each entity but flexible enough to disperse to

avoid defeat with the intent to disrupt command and control nodes is how the threat is adapting to power projection by the U.S. and her allies.

The likely implications for the future are, first, the information revolution will continue to favor networked organizations with flat command and control structures. Second, highly automated and hierarchical systems such as the U.S. will become more vulnerable to disruption from directed informational flows that seek to overload sensors and collection assets. Networks will conduct netwar from various locations in an attempt to influence perceptions and shape public policy. Traditional organizational structures as found in the U.S. military will have a difficult time fighting networked threats because of the threat's ability to rapidly form and disperse as the situation warrants.

Finally, it takes networks to fight networks. The future may require new organizations that are a hybrid of military units and non-military organizations working in conjunction to locate and counter networked threats. Experience indicates that for states with structures and institutions similar to the U.S., defense against networked threats will require effective interagency operations. Capabilities will be determined by the skillful blending of hierarchical structures with that of decentralized operations. "Netwar" and "networks" will significantly impact on the ability of the U.S. to project power in the future. Being the best at mastering the network medium will ensure that relative advantage on the battlefield is achieved.

BIBLIOGRAPHY

Adams, James. *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere*. New York: Simon & Schuster, 1998.

_____. "The Role of the Media." In *Cyberwar: Security, Strategy, and Conflict in the Information Age.* ed. Campan, Alan D., Douglas H. Dearth and R. Thomas Gooden. Fairfax, VA: AFCEA International Press, 1996.

Alexander, John B., COL, US Army (Ret). *Future War: Non-Lethal Weapons in Twenty-First-Century Warfare*. New York: St. Martins Press, 1999.

Arquilla, John. "The Strategic Implications of Information Dominance." *Strategic Review* XXII, No.3 (Summer 1994): 24-30.

Arquilla, John and David Ronfeldt. "A New Epoch-and Spectrum-of Conflict." In *In Athena's Camp: Preparing for Conflict in the Information Age*. ed. Arquilla, John and David Ronfeldt. Santa Monica, CA: RAND, 1997.

_____. *The Advent of Netwar.* Santa Monica, CA: RAND, 1996.

_____. "The Advent of Netwar." In *In Athena's Camp: Preparing for Conflict In the Information Age.* ed. John Arquilla and David Ronfeldt. Santa Monica, CA: Rand, 1997.

Bonisteel, Steven. "295 Mil Have Net Acess - Global Survey." On-line. Internet. Available from http://www.infowar.com/survey/00/survey_090800b_j.shtml: Inforwar.com, 12/2/00.

Bunker, Robert J. "Information Operations and the Conduct of Land Warfare." *Military Review* LXXVIII, No. 5 (September-November 1998): 4-17.

Clarke, Walter S. "Testing the World's Resolve in Somalia." *Parameters.* Vol 23. (Winter 1993-94): 42.

Cohen, William S. *Report of the Quadrennial Defense Review.* Washington, DC: Department of Defense, 1997.

Crock, Stan. "Sticks and Stones Can Break an Army." On-line. Internet. Available from http://www.businessweek.com/bwdaily/dnflash/oct2000/nf20001027_861.htm: Business Week Online, 12/2/00.

Daalder, Ivo H. and Michael E. O'Hanlon. *Winning Ugly: NATO's War to Save Kosovo.* Washington, D.C.: Brookings Institution Press, 2000.

Dunlap, Charles J., Jr. "Preliminary Observations: Asymmetrical Warfare and the Western Mindset." In *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?* ed. Matthews, Lloyd J., COL, US Army (Ret). Carlisle Barracks, PA: Strategic Studies Institute, 1998.

Evans, Michael. "Dark Victory: The Use of Military Force in Kosovo." *Working Paper No. 54.* (Canberra Australia: Australian Defense Force Academy, 1999).

Fast, William R., LTC, US Army. "Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age." On-line. Internet. Available from http://www.infowar.com/mil_c4i/00/ mil_c4i_071098d_j.shtml-ssi: Infowar.com, 12/2/00.

FitzSimonds, James R., Captain, USN. "The Cultural Challenge of Information Technology." On-line. Internet. Available from http://www.nwc.navy.mil/press/Review/1998/summer/art1su98.htm: Naval War College Review, 12/6/00.

Fox, John G. "Approaching Humanitarian Intervention Strategically: The Case of Somalia." In *Essays 2000: Chairman of the Joint Chiefs of Staff Strategy Essay Competition.* ed. General Henry K. Shelton. (Washington, DC: National Defense University Press, 2000): 36-38.

Glowacki, Victor. "Descent Into the Abyss: The Dangers of U.S. Intervention in Kosovo." On-line. Internet. Available from http://criterion.uchicago.edu//issues/April99/kosovo.htm: Newsweek, Inc., 12/3/00.

Goodwin, Brent Stuart. Review of "In Athena's Camp: Preparing for Conflict in the Information Age." *Naval War College Review.* Spring, 2000.

Gompert, David C. and Irving Lachow. "Transforming U.S. Forces: Lessons from the Wider Revolution." On-line. Internet. Available from http://www.infowar.com/mil_c4i/00/mil_c4i_103000a_j.shtml: Infowar.com, 12/2/00.

Harley, LtCdr. Jeffrey A., US Navy. "Information, Technology, and the Center of Gravity." *Naval War College Review* (Winter 1997): 1-19.

Huntington, Samuel P. *The Clash of Civilizations and the Remaking of World Order*. New York: Simon & Schuster, 1996.

Ignatieff, Michael. *Virtual War: Kosovo and Beyond*. New York: Metropolitan Books, 2000.

Johnson, Robert. "The Third Force: The Rise of Transnational Civil Society." On-line. Internet. Available from http://beta.ceip.org/files/Publications/thirdforcesummary.asp?p=10&from=pubdate: Carnegie Endowment for International Preace, 12/6/00.

Jones, Michael. "Internet Surfers Join Web War - War in Europe." On-line. Internet. Available from http://www.infowar.com/mil_c4i/99/mil_c4i_032999f_j.shtml: Infowar.com, 12/2/00.

Kaplan, Robert D. *The Coming Anarchy.* New York: Random House, 2000.

Kaplan, Robert et al. "Somalia Area Handbook." On-line. Internet. Available from http://lcweb2.loc.gov/c…cs:@field/DOCID+so0002. Washington, DC: U.S. Government Printing Office, SO0002-SO0131.

Kelley, Kevin. *Out of Control: The New Biology of Machines, Social Systems, and the Economic World.* New York: Addison and Wesley Publishing Co., 1994.

Keohane, Robert O. and Joseph S. Nye, Jr. "Power and Interdependence in the Information Age." *Foreign Affairs* 77, No. 5 (September/October 1998): 81-94.

Kitfield, James O. “Command and Control: The Messenger.” *National Journal* (September 11, 1999): 2546.

Kuehl, Daniel T. “Strategic Information Warfare and Comprehensive Situational Awareness.” In *Cyberwar: Security, Strategy, and Conflict in the Information Age.* ed. Campan, Alan D., Douglas H. Dearth and R. Thomas Gooden. Fairfax, VA: AFCEA International Press, 1996.

Lynch, April. "Kosovo Being Called First Internet War." On-line. Internet. Available from http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/04/15/MN38479.DTL: San Fransico Chronicle, 12/2/00.

Lyons, Terrence and Ahmed I. Samatar. *Somalia: State Collapse, Multilateral Intervention, and Strategies for Political Reconstruction*. Washington, D.C.: Brookings Institution Press, 1995.

Mahnken, Thomas G. "War and Culture in the Information Age." *Strategic Review* XXVIII, No. 1 (Winter 2000): 40-46.

McDonald, John W. “Exploiting Battlespace Transparency: Operating Inside an Opponent's Decision Cycle.” In *War In the Information Age: New Challenges for U.S. Security.* ed. Pfaltzgraff, Robert L., Jr., and Richard Shultz, Jr. Washington, D.C.: Brassey's, 1997.

McLendon, Col James W., USAF. "Information Warfare: Impacts and Concerns." On-line. Internet. Available from http://www.airpower.maxwell.af.mil/airchronicles/battle/chp7.html: United States Air Force Air University, 11/7/00.

Metz, Steven. *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*. Carlisle Barracks, PA: Strategic Studies Institute, 2000.

Miller, John H. “Information Warfare: Issues and Perspectives.” On-line. Internet. Available from http://www.ndu.edu/inss/siws/ch7.html.

Nuttall, Chris. "Kosovo Info Warfare Spreads." On-line. Internet. Available from http://www.infowar.com/mil_c4i/99/mil_c4i_041099c_j.shtml: Infowar.com, 12/2/00.

O'Neill, Richard P. “Integrating Offensive and Defensive Information Warfare.” In *War In the Information Age: New Challenges for U.S. Security.* ed. Pfaltzgraff, Robert L., Jr., and Richard Shultz, Jr. Washington, D.C.: Brassey's, 1997.

Paul, James A. "NGOs and Global Policy-Making." On-line. Internet. Available from http://www.globalpolicy.org/ngos/analysis/anal00.htm: Global Policy Forum, 12/2/00.

Pfaltzgraff, Robert L., Jr. and Richard Shultz, Jr. “Future Actors in a Changing Environment.” In *War In the Information Age: New Challenges for U.S. Security Policy*. ed. Pfaltzgraff, Robert L., Jr., and Richard Shultz, Jr.. Washington, D.C.: Brassey's, 1997.

Ronfeldt, David and Armando Martinez. “A Comment on the Zapatista Netwar.” In *In Athena's Camp: Preparing for Conflict in the Information Age*. ed. Arquilla, John and David Ronfeldt.. Santa Monica, CA: RAND, 1997.

Roxborough, Ian and Dana Eyre. "Which Way to the Future?" *Joint Force Quarterly*, No. 22 (Summer 1999): 28-34.

Scales, Major General Robert H. Jr., US Army. "From Korea to Kosovo: America's Army Learns to Fight Limited Wars In the Age of Precision Strikes." On-line. Internet. Available from http://www.afji.com/mags/1999/december/fromkoreatokosovo/index.html: Armed Forces Journal International, 11/7/00.

Scales, Major General Robert H. Jr., US Army. *Future Warfare: Anthology*. Carlisle Barracks, PA: U.S. Army War College, 2000.

Schwartau, Winn. *Cyber Shock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption*. New York: Thunder's Mouth Press, 2000.

Schwartau, Winn. “An Introduction to Infromation Warfare.” In *War In the Information Age: New Challenges for U.S. Security*. ed. Pfaltzgraff, Robert L., Jr., and Richard Shultz, Jr. Washington, D.C.: Brassey's, 1997.

Shukman, David. *Tomorrow's War: The Threat of High-Technology Weapons*. New York: Harcourt Brace & Company, 1996.

Stark, Rod. "Future Warfare: Information Superiority Through Info War." On-line. Internet. Available from http://www.infowar.com/mil_c4i/delphi.pdf: Inforwar.com, 11/15/00.

Steele, Robert David. "The Asymmetric Threat: Listening to the Debate." *Joint Force Quarterly*, No. 20 (Autumn/Winter 1998-99): 78-84.

Stevens, Alan. “Kosovo or the Future of War.” *Working Paper No. 54.* (Canberra Australia: Australian Defense Force Academy, 1999): 1-22.

Stein, George J. "Information War - Cyberwar - Netwar." On-line. Internet. Available from http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html: United States Air Force Air University, 12/2/00.

Szafranski, Richard. “A Theory of Information Warfare: Preparing for 2020.” In *Cyberwar: Security, Strategy, and Conflict in the Information Age.* ed. Campan, Alan D., Douglas H. Dearth and R. Thomas Gooden. Fairfax, VA: AFCEA International Press, 1996.

Thomas, Timothy L. "23 Human Network Attacks." On-line. Internet. Available from http://www.infowar.com/mil_c4i/00/mil_c4i_032100a_j.shtml: Infowar.com, 12/2/00.

_____. "Kosovo and the Current Myth of Information Superiority." On-line. Internet. Available from http://call.army.mil/call/fmso/fmsopubs/issues/kosovo.htm: Foreign Military Studies Office, Ft. Leavenworth, KS, 4/13/00.

_____. “Military and C4I.” On-line. Internet. Available from http://www.infowar.com/mil_c4i/00/mil_c4I_032100a_j.shtml: Infowar.com, 3/21/00.

Toffler, Alvin and Heidi Toffler. *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston: Little, Brown and Company, 1993.

U.S. Department of the Army. *Joint Vision 2020.* Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, n.d.

_____. *FM 3-0: Operations (DRAG Edition).* Washington, DC: Headquarters Department of the Army, June 2000.

_____. *FM 100-6: Information Operations.* Washington, DC: Headquarters Department of the Army, 1996.

Van Ripper, Paul K., LTG, USMC (Ret.) and LTC E.G. Hoffman, USMCR. “Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare.” *NSSQ,* (Summer, 1998), 1-19.

Verton, Dan. "DOD Redefining Info Ops." On-line. Internet. Available from http://www.fcw.com/fcw/articles/2000/0529/news-nato-05-29-00.asp: Federal Computer Week, 12/2/00.

Von Clausewitz, Carl. *On War.* ed. and trans. by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1975.

Waller, Douglas. “Public Affairs, Media, and War in the Information Age.” In *War In the Information Age: New Challenges for U.S. Security Policy.* ed. Pfaltzgraff, Robert L., Jr., and Richard Shultz, Jr. Washington, D.C.: Brassey's, 1997.

Weigley, Russell F. *The American Way of War: A History of United States Military Strategy and Policy.* Bloomington: Indiana University Press, 1977.

Weiss, Thomas G. *Military-Civilian Interactions: Intervening in Humanitarian Crisis.* New York: Rowman & Littlefield, Inc., 1999.

Woodward, Susan L. Failed States: Warlordism and "Tribal" Warfare. On-line. Internet. Available from http://www.nwc.navy.mil/press/Review/1999/spring/art2-sp9.htm: Naval War College Review, 12/6/00.