VOLUME III

INFORMATION AGE ANTHOLOGY:

The Information Age Military

EDITED BY

DAVID S. ALBERTS
DANIEL S. PAPP

CCRP

About the CCRP

The C4ISR Cooperative Research Program (CCRP) has the mission of improving DoD's understanding of the national security implications of the Information Age. Focusing upon improving both the state of the art and the state of the practice of command and control, the CCRP helps DoD take full advantage of the opportunities afforded by emerging technologies. The CCRP pursues a broad program of research and analysis in information superiority, information operations, command and control theory, and associated operational concepts that enable us to leverage shared awareness to improve the effectiveness and efficiency of assigned missions. An important aspect of the CCRP program is its ability to serve as a bridge between the operational, technical, analytical, and educational communities. The CCRP provides leadership for the command and control research community by:

- articulating critical research issues;
- working to strengthen command and control research infrastructure;
- sponsoring a series of workshops and symposia;
- serving as a clearing house for command and control related research funding; and
- disseminating outreach initiatives that include the CCRP Publication Series.

This is a continuation in the series of publications produced by the Center for Advanced Concepts and Technology (ACT), which was created as a "skunk works" with funding provided by the CCRP under the auspices of the Assistant Secretary of Defense (C3I). This program has demonstrated the importance of having a research program focused on the national security implications of the Information Age. It develops the theoretical foundations to provide DoD with information superiority and highlights the importance of active outreach and dissemination initiatives designed to acquaint senior military personnel and civilians with these emerging issues. The CCRP Publication Series is a key element of this effort.

Check our website for the latest CCRP activities and publications.

www.dodccrp.org

DoD C4ISR Cooperative Research Program

Assistant Secretary of Defense (C3I)

Mr. Arthur L. Money

Special Assistant to the ASD(C3I)
&
Director, Research and Strategic Planning

Dr. David S. Alberts

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors. They do not necessarily represent the views of the Department of Defense, or any other U.S. Government agency. Cleared for public release; distribution unlimited.

Library of Congress Cataloging-in-Publication Data

Alberts, David S. (David Stephen), 1942-
Volume III of Information Age Anthology: The Information Age Military
David S. Alberts, Daniel S. Papp
p. cm. -- (CCRP publication series)
Includes bibliographical references.
ISBN 1-893723-03-8

97-194630
CIP

March 2001

Volume III

Information Age Anthology:

The Information Age Military

Edited by

David S. Alberts
Daniel S. Papp

CCRP
Publication
Series

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The editors wish to thank and acknowledge the following publishers for granting permission to reproduce these important articles in *Volume III Information Age Anthology*:

"The War After Byte City" by Michael Vlahos, courtesy of the Center for Strategic and International Studies and the Massachusetts Institute of Technology from *The Washington Quarterly*, 20:2, Spring 1997

"Information Warfare in Multilateral Peace Operations: A Case Study of Somalia" by Rick Brennan and R. Evan Ellis, courtesy of Science Applications International Corporation, 1996

"Information-Based Warfare and the PRC" by M. Ehsan Ahrari, appeared as an earlier version of this essay as "Chinese Prove to be Attentive Students of Information Warfare," *Jane's Intelligence Review*, May 1997, and "U.S. Military Strategy Perspectives on the PRC: New Frontiers of Information-Based War," *Asian Survey*, December 1997

PREFACE

In what ways will wars and the Military that fight them be different in the Information Age than in earlier ages? What will this mean for the U.S. military?

In this third volume of the *Information Age Anthology*, we turn finally to the task of exploring answers to these simply stated, but vexing questions that provided the impetus for the first two volumes of the *Information Age Anthology*.

In Volume I, we examined some of the broader issues of the Information Age: what the Information Age is; how it affects commerce, business, and service; what it means for the government and the military; and how it affects international actors and the international system.

In Volume II, we turned to the impacts and consequences of the Information Age on national security broadly defined: the nature of national security in the Information Age, the threats to and opportunities for national security that may emerge in the Information Age, and differing interpretations about the degree of change in national security issues that we might expect to actually encounter in the Information Age.

Now, in Volume III, we concentrate on defense, conflict, and warfare in the Information Age. What characteristics will an Information Age military need to possess to meet current and future challenges? If so, how? What is the U.S. military establishment doing to prepare for change? How do military analysts in the United States view those changes? How are those abroad preparing their own military establishments for change? When all is said and done, what does all this mean for the defense of the United States and for its ability to deter and failing this, to prevail in the Information Age?

Given the uncertainties involved with the ongoing transition to the Information Age, the first two volumes provided us not with concise answers, but with some useful insights as to what the impacts and consequences of the Information Age may be on human affairs, commerce, business, the service industries, government, international actors, the international system, and national security affairs.

Similarly, Volume III is not meant to provide us with a textbook solution. Rather we hope that Volume III will provide us with improved insights and a sense of the direction that will serve us well on our journey to the future. We will continue to see through the glass darkly, but our aim is that the darkness will be several shades lighter than before.

CHAPTER 1

WAR IN THE INFORMATION AGE MILITARY

By
David S. Alberts and Daniel S. Papp

There is absolutely no doubt that advanced information and communication technologies and the capabilities that they impart will significantly change the nature of military roles, missions, and methods. Change will come not only to the militaries powerful nation states but to the militaries of smaller states and non-state actors. Around the world, defense strategists and planners are trying to puzzle out answers to the questions, "What will these changes be? How quickly will they occur? How can we manage the transition from where we are to where we need to be?"

These are not easy questions to answer. As we saw in Volume I of the *Information Age Anthology* and as everyday life at the beginning of the 21st century attests, the Information Age is ushering in major changes to virtually every human endeavor and undertaking. Volume II provided evidence that the nature of national security, how it is defined, how it is challenged and threatened, and how it is defended, is changing as well. In Volume III, we explore what Information Age technologies, their capabilities, and the age that they are ushering in may mean for militaries.

Precedents and Organization

Speculation about an impending “revolution in military affairs” began in the 1980s.[1] However, it was not until *Operation Desert Storm* in 1991 put the United States’ arsenal of precision weapons on display for Iraq to experience and the world to see that most people realized how far we had come technologically. In the months and years after *Desert Storm*, discussion, analysis, and speculation about the implications of Information Age technologies for warfare and conflict multiplied.[2]

Quickly, military scholars, analysts, and planners recognized that the implications of the new technologies for national security and defense policy extended far beyond precision force. As a result, defense doctrine began to be altered to take account of impending capabilities.[3] Meanwhile, fears multiplied about the threats of information and infrastructure warfare as more and more people recognized that Information Age technologies provided not only new capabilities but also created new vulnerabilities.[4] As new information and communication technologies entered the marketplace and the military at unprecedented speed, it sometimes seemed that the only thing that was keeping pace with the technologies was the uncertainty that they created about the future of national security and defense policy.

Just as Volume II of the *Information Age Anthology* examined the future of national security in the Information Age, this volume adds to the dialogue about defense policy by examining how militaries will change in the Information Age. This volume is organized into five parts:

The first part, "Strategy and Tactics," presents several views about how strategy and tactics might evolve in the Information Age. The only thing these authors can agree on is that strategy and tactics will change. They agree on nothing else. One article posits that changes in defense policy will be small and incremental but accelerate, while another argues that changes will be massive and potentially cataclysmic. A third article examines the future of deterrence, and a fourth explores alternative visions of future war.

The second part, "Official Service Perspectives," reviews how the U.S. Joint Chiefs of Staff, the four armed services, and the Office of the Secretary of Defense see the future of warfare and conflict and are preparing American forces to fight. On the surface, significant agreement exists, but below the surface, disagreements are apparent both about the future of warfare and about how best to prepare.

The third part, "Believers and Skeptics," presents views on the impact of Information Age technologies on defense policy. Three views differ considerably. Two accept that the new technologies will provide significant advantages to American armed forces, and look forward to that future. One author is concerned that the technologies and their capabilities are being over-sold. While the fourth author raises what he believes are serious questions not only about present operational capabilities but also about the significant limitations of the technologies.

The fourth part examines the nature of future warfare. The first article develops a nightmare scenario of asymmetric warfare based on information technology, stealth, and biological weapons in which the leadership of the United States is decapitated. The second explores the threat that sub-state groups could present to the U.S. and other developed states. The last three articles examine how broadly defined information operations were used in Somalia, Bosnia, and Kosovo.

The fifth part presents perspectives on how selected NATO states, Russia, and China view the impact of Information Age technologies on defense policy and how they are responding to its challenges. Not surprisingly, a number of perspectives are quite different from those held in the United States. But similar viewpoints exist on some issues as well.

The volume concludes with the views of the editors on what can be expected to happen in the first few years of the 21st century.

In this introduction to Volume III, we set the stage. We note that the definitions for key terms are still in the process of evolution.

Second, we explore the changing context. Simply put, information is becoming a more important factor in the creation of wealth. Second, information is becoming a commodity. Third, the increasing importance and value of information is leading to both organizational and valuative changes to societies and of course to their militaries.

Third, we discuss the following. We identify six consequences of the Information Age that will have profound effects on militaries:

1. Time and distance will become less important as constraints.

2. More international actors will affect events.

3. Boundaries between international actors will become more permeable.
4. Democratic governments and free market economies will flourish, but not become the only forms of government or economic organization.
5. Trends toward regionalization and globalization will accelerate.
6. The disparity between haves and have-nots will increase.

The fourth section of this introduction to Volume III provides an examination of the sources of potential threats. Not as detailed as the discussion of challenges and threats to national security contained in Volume II of the *Information Age Anthology*, this discussion stresses that threats may come from more diffuse sources and that asymmetric warfare presents a real—although not new—security danger.

We conclude our introduction by pointing out that, as important as Information Age technologies are in inducing change, they are not the only technologies that are experiencing sizeable advances. Thus, the real revolution in military affairs may well arrive when advanced information and communication technologies are combined with the many other technologies that are advancing rapidly and which have military applications.

What Are We Actually Talking About?

At first blush, the answer to this question is self-evident. Obviously, we are talking about the opportunities that advanced information and communication technologies—

that is, Information Age technologies—provide to militaries to improve the way they organize, equip and fight.

Specifically we are talking about sensors, radar, and other information collection devices are being improved on almost a daily basis. These improved collectors are increasingly capable of being networked together to provide military commanders with an enhanced awareness of the battlespace including Global Positioning Systems allowing even individual soldiers to know precisely where they are. And we are talking about highly reliable high-speed global communications systems, including space-based components, that provide the opportunity to communicate this enhanced battlespace awareness to any point on the planet where it is needed. Advanced information and communication technologies are the basis for precision strike capabilities that improve lethality while minimizing minimizing collateral damage. And once a strike of any kind is delivered, Information Age technologies provide the ability for better battlespace damage assessment, which increases both effectiveness and efficiency.

Accompanying these opportunities for improvement is a greatly increased need or “Information Operations” that can protect one’s own information and destroy an enemy’s information, thereby rendering his military forces degraded or inoperative and his society and government weakened and undermined. Much of course has already been written about these new capabilities. Many “new terms” have been coined, re-coined and used somewhat inconsistently in the literature including: “system of systems,” “information operations,” “information superiority,” “information warfare,” “network-centric warfare,” and “the revolution in military affairs." Somehow, it is assumed that everyone knows precisely what these terms mean.

This occurs in casual conversation, arcane analyses, and Defense Department documents. Specifically, beyond the debates over the meaning and use of "revolution in military affairs,"[6] in the meaning and use of the terms "information operations" and "information superiority" generate the most discussion.

While some decry this lack of clean, clear unambiguous and fully agreed to definitions of key terms, we see this as an essential part of discovery, exploration and progress. After all, we are just beginning to come to grips with the Information age and not recalling it in retrospect. The following is the current state of our efforts to come to grips with the meaning of two of the central concepts.

At the Joint Chiefs' level, definitions of "information operations" and "information superiority" are clearly set forth. Information operations is defined by US Joint Publication 3-13, *Joint Doctrine for Information Operations*, as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[7] The same publication defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[8]

As straightforward as these definitions appear, at the service level, they provide room for different interpretations to be developed. The Army and the Navy, for example, have different views of what is included within information operations.

According to the U.S. Army's Field Manual *FM 100-6*, information operations refers to operations linking together public affairs, civil affairs, psychological operations, command and control warfare, and electronic warfare.[9] This is a broad definition of information operations. Even so, all elements of the Army's definition arguably fall within the Joint Chief's definition. At the same time, all elements of the Army's view of what is included within information operations have been affected and are being affected by advanced in information and communication technologies.

Conversely, the Navy's view of what constitutes information operations is more restrictive. According to the Navy's *Information Warfare Strategic Plan*, information operations include only those actions taken "to exploit the opportunities and vulnerabilities inherent in the dependence on information to support military activities." Continuing, the Navy's *Strategic Plan* maintains that information operations "include actions taken to affect an adversary's information and information systems, and those taken to protect U.S. information, information-based processes, and information systems."[10] While the Navy's definition does not specifically preclude public affairs, civil affairs, and psychological operations, all elements which are included by the Army, the Navy's understanding of and orientation toward information operations clearly is more narrowly defined than the Army's.

The *Quadrennial Defense Review*'s discussion of information operations does little to reduce the inconsistency between the Army's and Navy's viewpoint. The *QDR* declares that the Defense Department has "directed most of its efforts in [information operations] toward protecting critical U.S.

infrastructure against hostile information operations and developing U.S. information operation capabilities for use in peacetime engagement activities, smaller-scale contingencies, and major theater wars." The *QDR* also notes that one of the Defense Department's highest priorities "will be the institutionalization of information operations—that is, the integration of information operations concepts into military planning, programming, budgeting, and operations."[11] While the *QDR*'s discussion implies that a broad definition of information operations is legitimate, room for interpretation remains.

These differences spill over into the meaning, implications, and operational significance of information superiority. For example, the Department of Defense's 1999 publication *Information Operations* maintains that information superiority is based on U.S. dominance in intelligence, including surveillance and reconnaissance; command, control, communications, and computers; and information operations. At the same time, it states that "information operations and information superiority are at the core of military innovation and our vision for the future of joint warfare….The capability to penetrate, manipulate, and deny an adversary's battlespace awareness is of utmost importance."[12] It also declares that "the chief concern of information superiority is the human user of information. Without knowing when, where, why, with what, and how to act, warfighters cannot perform mission-essential tasks efficiently and effectively."[13]

But *Information Operations* does not clarify the disagreement between the Army's and the Navy's definition of information operations, nor does it clarify what the boundaries of the battlespace may be. And as applied to information superiority, this has clear operational significance.

This point was driven home by General Wesley Clark, Supreme Allied Commander Europe, during his Fall 1999 testimony to the Senate Armed Services Committee. Clark reportedly questioned the need for the bombing campaign against Serbia, opining that NATO could have used “methods to isolate Milosevic and his political parties electronically.” Continuing, Clark asserted that if electronic means had been used in conjunction with other non-military measures, the military assault might not have been necessary.[14]

We still have a ways to go in developing one of a shared (at least within the U.S. defense establishment) and set understanding of what these terms mean and what they imply. One of the first tasks at hand is therefore to develop a shared (at least within the U.S. defense establishment) set of definitions of what these terms mean and what they imply. We will be able to measure our progress by the evolution of these terms and our ability to build a consensus regarding their meaning and their implications.

The Context of Defense Policy in the Information Age

As Volume I of the *Information Age Anthology* illustrated, the Information Age is changing virtually all human endeavors and undertakings. This in turn means that, as Volume II of the *Information Age Anthology* showed, concepts of national security are changing. This leads to the reality that the context within which defense policy is pursued is changing.

These changes have many different dimensions, but only three will be discussed here.

First, in the Information Age, information is becoming an increasingly important to the creation of wealth, power, and influence. In many peoples' eyes, information has already become more important than the traditional sources of wealth: land, labor, and capital. Information is something to be prized both for what it is and what it can do.

Regardless of the current value of information, its importance relative to land, labor, and capital will continue to increase. This means that the traditional sources of wealth and power will become relatively less valuable, perhaps even losing most of their value. At some point they may not be worth fighting for.

What does this mean for defense policy? Put simply, to the extent that defense policy deals with defending and/or securing the foundations of national wealth, power, and influence, defense policy must change to include the defense and/or securing of information. It also means that defending the traditional sources of wealth and capital will become a relatively less important function of defense policy.

Many questions spring from these Information Age "facts". Which information, required and valued by whom, should be defended or secured? Who should make the decision to defend and/or secure information? When a decision is made, what is the best way to achieve the objective, and what will be required to achieve it? Which land, labor, or capital is relatively less important, and what steps should be taken, or not taken, to defend and/or secure it? Many of these and other related questions are the same as or similar to those asked by defense analysts and strategists before the Information Age. However, the answers will now be different.

The answers will be different not only because of the increasing absolute and relative importance of information, but also because other values will change. The relative values attached to the individual, the family, and society; to materialism, secularism, and religion; to honor, duty, and country; and to many other values will inevitably become different as we are bombarded by more and more information. Unfortunately for all of us, but especially for defense planners and strategists, it is not possible to predict what the changes will be.

Will the lives of friendly forces be valued so highly that casualties in conflicts will not be accepted? Will it still be worth fighting for territory and/or resources? Which territory, and what resources? Will large defense budgets, or even moderately sized ones, be politically possible? Will main force conflict be rejected as unacceptably destructive? Will wars over information and attacks on information be politically acceptable? Just as universal service versus the all volunteer armed forces, race relations, the role of women in the military, and sexual harassment were among the valuative questions of the late Industrial Age, these may be the valuative questions of the early Information Age.

The Information Age has already begun to induce change in organization and structure in other areas of society, the military will experience organizational and structural change. Many corporate organizations and structures have been flattened, with direct lines of reporting between operational arms and agencies and decision makers being put in place. Often, increased decisionmaking authority has been delegated to operational arms and agencies. Many businesses have opted for partnerships with others in the same or related business sectors, even with competitors, with some predicting that "co-opetition" will become the order of the day in the Information Age business world.

Many of these same trends have begun to appear in the U.S. military. Although the organization and structure of the U.S. military and its formal lines of reporting have not changed, information flow among levels has accelerated, achieving a somewhat similar affect. Command and control remains critically important, but the need for quickly made on-the-scene decisions is widely recognized. One reflection of this is the U.S. Marines' replacement of "command and control" with "command and coordination." *Joint Vision 2010*'s emphasis on combined operations and jointness is in many respects the military equivalent of "co-opetition." It is too soon to say how far these changes may go, but they may be extensive.

Amid our emphasis on capabilities and doctrine, then, we can not lose sight of the fact that the context of defense policy is changing. The implications of this are considerable. In the Information Age, military objectives may be different. The societal values in which the military is immersed and on which the military is based may be different. And despite tradition, the organizational structures on which the military is based may have to be different if the best defense policy possible is to be implemented.

The Strategic Environment and Defense Policy

In addition to the changes that the Information Age is inducing in individual human endeavors and undertakings, it is also altering the global international system, the structure of the system, and the way that the system works. As a result, the strategic environment within which defense policy will be pursued will change, perhaps drastically. These changes will have sizeable implications for defense policy.

Time and Distance Will Constrain Less Than in the Past

One of the chief hallmarks of the Information Age is that the relevance of time and distance as constraints on human activity and productivity will be sharply reduced. With more and more types of messages and information travelling at the speed of light over long distances with little or no loss of clarity, accuracy, or meaning, time and distance are becoming less and less restrictive on many forms of human activities and capabilities.

The implications of this for defense policy are contradictory. On the one hand, as bandwidth and reliability increase and it becomes increasingly possible to flash information about developing situations in real time from the point of contact to a command authority, it could mean that command and control becomes increasingly centralized. This may be especially true in highly sensitive situations.

Conversely, the flood of information that increased bandwidth and reliability will provide to command authorities may dictate that more and more decisions be made on the ground at points of contact. As more detailed information about more and more tactical situations becomes available to a command authority, it may become more and more difficult for the command authority to remain focused on the theater or strategic pictures. The combination of more information available at the tactical level and too much information at the operational level may thus drive more decisionmaking to the tactical level.

Either eventuality implies that organizational structures in the military, as has already happened in many industries, will be flattened. Hierarchy will remain, but it is likely that the number of levels between top and the bottom will decrease.

More International Actors Will Have the Ability to Affect Events

The strategic environment of the Information Age will also be changed by a proliferation of international actors that could play a major role in affecting events. Many factors contribute to this phenomenon, but Information Age technologies are among the most prominent.

The proliferation of potentially prominent international actors is taking place in two ways. First, advanced information technologies are expanding the role that multinational corporations, non-governmental organizations, and even individuals play in the international arena. Second, as Information Age technologies permeate human affairs more and more widely, more and more businesses, non-governmental organizations, and individuals are empowered to involve themselves in the international arena in meaningful ways.

This has immense, but again uncertain, implications for defense policy. As more and more actors gain potential to have major impacts on the national interests of a state, will a state's command authority be able to identify those actors who present a serious threat to its interests? Will the command authority be able to differentiate between serious threats and dangers that are merely modest challenges? Will the command authority be able to differentiate between challenges and threats to its own interests and challenges and threats to the interests of other actors such as MNCs? If it can not, will it view threats, challenges, and pranks with an identical degree of concern?

These are critical issues, and they are not necessarily new in the realm of defense policy. However, given the decreased relevance of time and distance as constraints, the urgency of answering them will be greater in the Information Age than ever before. We will return to these issues later.

Information Flows Ignore National Boundaries

The nature of modern networked systems and other information and communication technologies is such that the flow of information can be curtailed with only great difficulty, and sometimes not at all. This reality is a two-edged sword.

On the one hand, it means that all types of intercourse between international actors will increase. This bodes well for democracy and markets, as will be discussed below.

Conversely, it also means that information some deem unacceptable or unfavorable can spread easily. Recognizing this, some governments have resorted to Internet-explicit licensing and regulation, filtering content, and or restricting or denying access to the Internet in particular. For example, the U.S. government in 1996 tried to control the presence of pornography on the Internet with the Communications Decency Act, which was eventually ruled unconstitutional. More broadly and more seriously, at least twenty governments totally or mostly control access to the Internet to “protect traditional values,” “defend national security,” “promote morality,” or “prevent the spread of subversion.”[15]

The permeability of national boundaries also means that the disruption or corruption of information flows can spread widely and rapidly, as evidenced by global impact of the May 2000 “Love Bug” worm. Launched from a single computer in the Philippines, the worm and its 29 or more variants reportedly caused over $10 billion of damage worldwide before it was substantially corralled.[16] Even though warnings about the worm were broadcast within a few hours of its identification, its victims included most Fortune 500 corporations, at least fourteen U.S. government agencies including the Department of Defense, agencies of several non-U.S. governments, and millions of private individuals around the world.

Maintaining secure information and computer systems must be a high priority in the Information Age. The increased permeability of boundaries among international actors raises the stakes of security still higher. This clearly has immense importance for defense policy. The elements of such security are worth repeating here.

First, the ability to identify intrusions into and other electronic assaults on information and information systems must be in hand. If it is not, it must be developed. A perpetual race between information security and threats to information security is already well underway. At the same time, as already stated, the ability to differentiate between threats, challenges, and pranks is also needed.

Second, the ability to identify threats to information and information systems is not enough. Such threats must be identified quickly. For example, in February 2000, a series of distributed denial of service attacks against Amazon.com, Yahoo!, CNN.com, and E-trade caused millions of dollars of losses. The technology was on hand to identify these attacks more quickly, but it was not well employed or monitored. Had these attacks been identified quickly and appropriate counter-measures initiated, the damage they caused could have been significantly curtailed.

This then leads to the final point, the requirement that effective and appropriate counter-measures be used immediately when a threat is identified. Using the Love Bug as an example, even though it was identified as a threat rather quickly, the warnings that went out in response to it proved only marginally effective in curtailing the damage that it caused. And using the February 2000 distributed denial of service attacks as an example, the slow rate of response led to extensive financial loss even though tools were in hand to cope with the attack.

In the globally networked environment of the Information Age, the increased permeability of the boundaries among international actors requires information security measures that are reliable, discriminating, rapid, and effective.

Democratic States and Free Markets Economies Will Flourish

Although claims that the Information Age favors democratic forms of government and free market styles of economic organization often go beyond what documented evidence supports, there is logic to the argument that the free flow of information enhances human freedom and productivity. It also follows that any political or economic system that encourages the free flow of information enjoys an advantage in comparison to those that do not. It is likely, then, that the most successful international actors of the Information Age will be democratic states with market economies.

But not all states or other international actors will be democratic or market-oriented. As we have already seen, some states, and on occasion other international actors as well, will attempt to restrict, deny, or otherwise curtail access to information technologies and the capabilities that they afford, arguing that they are protecting traditional values, defending national security, promoting morality, or preventing subversion.[17]

In addition, isolated outposts of like-minded individuals and groups who oppose democracy and free markets may use Information Age technologies to band together to further their own purposes. So too will other interest groups. Sometimes, these other interests will inevitably conflict with the interests of democratic free market states.

For defense policy, then, even though the successes of democratic free market states will lessen many traditional national rivalries, defense forces will not want for activity. Democratic states and free market economies may flourish in the Information Age, but new challenges and threats will arise, and many traditional challenges and threats will remain and perhaps grow. For defense policy, the Information Age will provide more challenges than ever.

The Trend Toward Regionalization and Globalization Will Accelerate

The ability to transfer information regionally and globally at a moment's notice will accelerate the drive toward regionalization and globalization. The rapid transfer of information enables the creation of distributed production systems that extend beyond localities and states to entire regions and even the world, thereby, at least in theory, driving down production costs as businesses take advantage of lower production costs that exist beyond local or national boundaries.

Without denying the importance of the transformed post-Cold War political climate in accelerating regionalization and globalization, the true enablers of regionalization and globalization have been advanced information and communication technologies. The European Union, MERCOSUR, ASEAN, the Free Trade Area of the Americas, and APEC all do benefit or will benefit immensely from these Information Age technologies.

For defense policy, the accelerated trend toward regionalization and globalization has one major implication. As the economies and other interests of states become increasingly intertwined, so too will their defense policies. In some instances, this will present no real problems politically or operationally. In other instances, this will not be the case. For example, questions already exist about whether the gap between the technological prowess of the United States' armed forces and the armed forces of U.S. allies is so great that meaningful military cooperation is precluded. Most analysts believe that this gap will increase even further.

The Disparity between Haves and Have-Nots Will Increase

As those who know how to use advanced information technologies within both advanced and developing countries employ those technologies, their wealth will accumulate more rapidly than the wealth of those who are technologically incapable. Thus, to the extent that information technologies will be diffused and used in different societies at different rates of speed, and to the extent that those technologies create wealth, they will tend to increase the degree to which there is a skewed distribution of wealth.

This phenomenon will occur both within and between countries. Even within countries that are currently underdeveloped, a segment of the population may be expected to learn how to use and benefit from Information Age technologies. This will skew distributions of wealth within those countries even more than they are today. At the same time, it is reasonable to expect that countries that are currently economically advanced will for the most part benefit the most and the soonest from advanced information technologies. Thus, disparities in the distribution of wealth between have and have-not countries may be expected to increase as well, as least during the early years of the Information Age.

A fortunate few countries blessed by enlightened leadership, advanced education, or good fortune may use information technology to progress more rapidly than others. These few countries may even succeed in closing the economic gap between themselves and richer states. But these countries will be the exception rather than the rule.

If the gap between rich and poor increases, resentment of the poor against the wealthy may increase, leading to unrest within states and tension between states. Instead of ushering in an era of peace and prosperity, Information Age technologies could lead to rising domestic unrest in some states and growing international tension between others.

From Where Will Challenges and Threats Arise?

One of the hallmarks of the Information Age will be increasingly available and increasingly affordable information and information technology. In some cases, information and information technology will be applied to existing weapons and weapon systems to enhance their capabilities ("information enhanced weapons"). In other cases, information and information technology will become so central to the functioning of a weapon or a weapon system that the weapon or weapons system will not be able to function in its absence ("information enabled weapons"). In still other cases, the increased reliance of civil societies on information and information technologies will render them vulnerable to attacks against its information and information technologies by new and innovative weapons (“information warfare”).

More Actors as Challengers and Threats

What is more, advances and breakthroughs in information and communication technologies can often readily be achieved by small teams of researchers, or even individuals. Sometimes, advances and breakthroughs may be achieved using relatively inexpensive “off-the-shelf” technology available from commercial vendors. In both cases, advances and breakthroughs can sometimes be translated by potential enemies into challenges or threats.

This is different than during the Cold War when the generation of sizeable challenges or threats to the national interests of major state actors required adversaries to marshal large quantities of resources to develop and deploy nuclear weapons, air armies, tank divisions, and aircraft carrier battle groups. Thus, during the Cold War, sizeable challenges and threats to the interests of major states could usually be generated only by other major states.

In the Information Age, this will no longer be true. The increased availability and affordability of information enhanced, information enabled, and information warfare capabilities will allow more international actors, including non-state actors, to present more diversified and viable threats to the interests of major state actors, including the United States.

Asymmetric Warfare as a Threat

Asymmetric warfare is the “enfant terrible” of the early 21st century. Most often defined as warfare in which an enemy resorts to the use of weapons of mass destruction, terrorism, urban or guerrilla warfare, or information warfare, the dangers of asymmetric warfare are real and should not be minimized.

At the same time, asymmetric warfare is not something new or revolutionary. Hannibal chose to drive his elephants through the Alps rather than confront Rome directly. Giap chose to resort to hit-and-run jungle warfare rather than confront Westmoreland’s main force divisions directly. And Schwartzkopf chose his end around strategy to avoid assaulting Saddam’s bombed out but dug in forces directly. Throughout history, wise military leaders have adopted strategies that minimized enemy strengths and maximized their own ability to exploit enemy vulnerabilities.

Military strategy in the Information Age will be no different, regardless if it is employed by “peer competitors” that are major state actors, “niche competitors” that are small state actors or non-state actors, or any of a variety of lesser challenges that may spring up. Almost all will adopt strategies that seek to minimize the strengths of the United States and its friends and allies and exploit their vulnerabilities, regardless of the extent to which Information Age technologies enhance, enable, or create U.S. and friendly military capabilities.

Without minimizing the level of threat that asymmetric warfare presents, it must be recognized that asymmetric warfare is a rediscovered reality of military affairs. It is not a function of the Information Age.

Other Voices: Defense Policy and Technological Advances in Fields Beyond Information Technology

As important and significant as the advances in Information Age technologies are, they are not the only technologies rapidly advancing. Other “high tech” fields are also experiencing rapid advances, and many have extensive implications for defense policy. It would be a serious error to restrict analysis of the future of defense and defense policy to those induced exclusively by advanced information and communication technologies.

Impressive advances are being made in technologies such as directed energy, stealth, robotics, miniaturization, micro-electro-mechanical systems (MEMS), biotechnology and bioengineering, molecular biology, non-human behavioral modification, materials, and nanotechnology. Individually, several of these technologies have extensive military utility and implications. When they are combined, they promise to provide the military forces that obtain them the ability to engage in warfare, conflicts, and operations other than war in truly revolutionary ways.[18]

Indeed, some of the military systems that today can be realistically envisioned were in the not-too-distant past the stuff of science fiction. Low-cost sensors disguised as grass or sand are on the horizon. Defensive systems deployed as aerosols will also soon be available. So too will focused long-range laser systems with extensive destructive potential. Insects and animals may soon be used as trackers and sensors, while cyborg systems that combine mechanical structures and living organisms for military purposes are further in the future. Nevertheless, they are there, as are fully roboticized military systems that completely remove humans from the loop. None of these concepts are too far over the horizon.

What will happen to defense capabilities and defense policy when these technologies are combined with those of the information revolution? The possibilities are immense. The Information Age is only beginning.

[1] For a discussion of debates among proponents of the revolution in military affairs, as well as an analysis of why present advances in military capabilities do not represent an RMA, see Stephen Biddle, "The Past as Prologue: Assessing Theories of Future War," *Security Studies* (Autumn 1998), pp. 1-74.

[2] See, for example, Michael J. Mazarr, Jeffrey Shaffer, and Benjamin Ederington, *The Military Technical Revolution* (Washington, D.C.: Center for Strategic and International Studies, 1993); Williamson Murray, "Thinking About Revolutions in Military Affairs," *Joint Forces Quarterly* (Summer 1997); and Colin Gray, "The American Revolution in Military Affairs: An Interim Assessment," *The Occasional, Number 28*, (Strategic and Combat Studies Institute, September 1997); and Stuart J.D. Schwartzstein (ed.), *The Information Revolution and National Security: Dimensions and Directions* (Washington, D.C.: Center for Strategic and International Studies, 1996).

[3] See the excerpts from *Joint Vision 2010* and related service and Office of the Secretary of Defense documents, Chapters 6-12 in this volume.

[4] See James Adams, *The Next World War: Computers are the Weapons & the Front Line is Everywhere* (New York: Simon & Schuster, 1998); John Arquilla and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997); Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND, 1996); Winn Schwartau (ed.), *Information Warfare* (New York, NY: Thunder's Mouth Press, 1996); and and William H. Webster, Arnaud de Borchgrave, et al., *Cybercrime...Cyberterrorism... Cyberwarfare...Averting an Electronic Waterloo* (Washington, D.C.: Center for Strategic and International Studies, 1998).

[5] See Daniel S. Papp and David S. Alberts, "National Security in the Information Age: Setting the Stage," in Daniel S. Papp and David S. Alberts, *Information Age Anthology, Part II: National Security Implications of the Information Age*, Chapter 1, for a thorough discussion of the relationship between defense policy and national security. See also Peter L. Hays, et al., "What Is American Defense Policy?," p. 9, in Peter L. Hays, et al. (eds.), *American Defense Policy, Seventh Edition* (Baltimore: The Johns Hopkins University Press, 1997), for a discussion of defense policy.

[6] See again Biddle, "The Past as Prologue: Assessing Theories of Future War," pp. 1-74.

[7] US Joint Chiefs of Staff, Joint Publication 3-13, *Joint Doctrine for Information Operations* (Washington, D.C.: U.S. Government Printing Office, October 1998), p. II-10. GL-7. See also Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* (Washington, D.C.: U.S. Government Printing Office, n.d.)

[8] *Joint Doctrine for Information Operations*, p. GL-7.

[9] U.S. Army, *Field Manual FM 100-6*.

[10] See the U.S. Navy's *Information Warfare Strategic Plan*, Chapter 10 in this volume.

[11] See *Quadrennial Defense Review*, Chapter 12 in this volume.

[12] U.S. Joint Chiefs of Staff, *Information Operations*, March 1999, p. 1.

[13] *Ibid*., p. 6.

[14] Julian Borger, "Cyberwar Could Spare Bombs," *The Guardian*, November 5, 1999, p. 17.

[15] These countries include Azerbaijan, Belarus, Burma, China, Cuba, Iran, Iraq, Kazakstan, Kyrgyzstan, Libya, North Korea, Saudi Arabia, Sierra Leone, Sudan, Syria, Tajikistan, Tunisia, Turkmenistan, Uzbekistan, and Vietnam. See *Censor Dot Gov: The Internet and Press Freedom 2000* (New York, N.Y.: Freedom House, 2000).

[16] See http://www.nipc.gov

[17] See again Footnote 15.

[18] See Steven Metz' "Military Strategy and Information Technology: Alternative Visions of Future War," Chapter 5 in this volume, for a more detailed discussion of many of these technologies.

PART ONE

INTRODUCTION

How will the Information Age change what the military will do and how it does it? The five articles in this section examine this question from a variety of different perspectives and reach widely different conclusions.

The first sees the Information Age ushering in an era in which national grand strategy must change, but is optimistic that a workable new grand strategy will emerge. The second is much more pessimistic. It argues that the Information Age is initiating changes in society and warfare so far-reaching and fundamental that little is predictable. The third also raises a major concern. It argues that even though a major war remains unlikely, the Information Age is weakening deterrence. The fourth postulates that new technologies will change the ways that wars are fought more fundamentally than is widely recognized and is currently reflected in our thinking about the future. Despite this, it is optimistic about the ability of the United States and the American military to initiate the required fundamental changes. The final article, pointing to the immense information requirements required by emerging operational concepts and to the vulnerabilities created by required linkages between sources of information, is skeptical about whether an information induced Revolution in Military Affairs (RMA) is possible.

In the first article, “Grand Strategy and Information Warfare,” Daniel Goure presents an optimistic assessment of the impact of the Information Age on U.S. interests and global security. Beginning with the observation that “the purpose of grand strategy is to organize the power available to the state in such a way as to ensure national survival, the well being of the people, and the maintenance of national institutions,” Goure observes that the Information Age (or as he terms it, the Information Revolution) has already changed the definition of power available to the state, and may also be altering the meaning of the well being of the American people and the requirements for the maintenance of national institutions.

What does this mean for grand strategy? Observing that most analyses of the impact of the Information Age on warfare concentrates on information as a force multiplier, Goure presents a persuasive case that the Information Age will make major wars less likely. “How can you hoard information?”, the author asks. “How can you fight for information?”, he continues. And given that from his perspective the state will be the major player in international affairs long into the Information Age, what will the cause of major war be? Few exist, he maintains, so major wars will become less likely.

However, Goure stresses, the ground will be open for “lesser conflicts of serious note.” But these conflicts will be limited in scope, scale, or objective, he predicts. U.S. force planning must change to accommodate this probability, he argues, but at the same time, this means that potential adversaries will probably change their strategies, concentrating on the acquisition of weapons of mass destruction and long-range ballistic missiles to complicate the ability of the United States to project power into their region.

This means, Goure asserts, that with its global interests, the U.S. must cultivate and maintain friends and allies throughout the world in regions in which it has interests by contributing to their security. In the Information Age, he says, the U.S. is likely to "find itself the guarantor of the freedom of all the lines of global communication and power." And this, he asserts, is a source of enormous potential power.

The implications of this for U.S. grand strategy are far reaching. Current warfighting doctrine, even those modernized under the auspices of *Joint Vision 2010* and the various follow-on service documents, may no longer be relevant, he believes. Obtaining classical objectives via a series of battles is becoming politically less important, Goure observes, even as the importance of launching a devastating first salvo under severe political and operational constraints becomes greater. Strategic intelligence therefore is becoming more important, Goure argues, and he concludes that a combination of anti-access strategies and CCD may be the best way for a potential enemy to "thwart a U.S. military strategy based on…information superiority."

What, then, should U.S. grand strategy be in the Information Age? Goure offers several answers. For example, he says, the U.S. must concentrate more on correlating data and interpreting it than on collecting more of it. Similarly, he posits, the U.S. needs to gather and process enough information so it can understand and manipulate macro-level phenomenon such as group psychology and economics. Perhaps most importantly, he maintains, the U.S. must develop a grand strategy of being the ally of choice in regions where it has interests by sharing technology and know-how, and in so doing, helping to create a vibrant and growing global infosphere. This is well within U.S. capabilities and vital to U.S. interests, Goure concludes.

In the second article in this section, “The War After Byte City,” Michael Vlahos is much less optimistic about whether the U.S. and its military establishment, or for that matter the political-military leadership of any country, can cope with the challenges of the Information Age. Vlahos reaches this pessimistic conclusion for a simple reason. “Big Change” is coming, Vlahos insists, driven by the technologies and the capabilities of the Information Age, and the implications of “Big Change” for society and war are immense.

What exactly does Vlahos mean by “Big Change?” In basic terms, he argues that the Information Age is bringing with it not only new technologies and new capabilities, but also new patterns of relationships between and within societies. These new patterns of relationships, he asserts, will lead to a global systemic breakdown, beginning with the global economy. This economic revolution, he predicts, will tear old ways of life apart and bring upheaval to world cultures.

To Vlahos, the Internet and its associated technologies are what is driving Big Change. Time and distance will cease to be barriers. Knowledge will provide value, and the marketplace will determine value. These facts, as Vlahos sees them, will overthrow the way that things have been organized and undertaken not only in the U.S., but throughout the world.

As ill prepared as Vlahos believes the United States is for Big Change, he sees the rest of the world, including Japan and Europe, as even less prepared. In every part of the world, Vlahos maintains, there will be some people who will adapt to change, and others who can exploit change for their own purposes. Many of these people will look at the world differently than today's main players do. They will think differently and have different value systems. And they will organize themselves differently as well. Some will create new ideologies, which to Vlahos will be "new religions" that have a "passionate conviction that their truth is the only truth."

Who will adapt to change, who will develop "new religions," and who will pose threats to the established ways of doing things? Vlahos does not know. "The next enemy," he says, "does not yet exist." It will not be a "big place of industrial iron" like China, nor necessarily a "dynamic small place" like Singapore. Rather, potential challengers to established ways of doing things and organizing things may well spring from non-state sources, he says. They will be unified by ideas not by geography, and as such, they will be impossible to counter or control, at least by current military power.

To Vlahos, the U.S. and the rest of the global establishment are not ready or able to think in terms of challenges arising from non-state, perhaps even post-state, sources. Vlahos offers what he believes are three proofs of this, the U.S. military's emphasis on:

1. readiness, which he decries as locked into a "fighting the last war" mentality;

2. reform, which he dismisses as an inadequate effort to improve bureaucratic performance by improving efficiency; and

3. (r)evolution, which he charges simply replaces old weapons with new weapons when what is needed is replacing old thinking with new thinking.

Vlahos concludes pessimistically. We can prepare for future conflict, he asserts, but the changes that the Information Age is ushering in are so all-encompassing, pervasive, and revolutionary that we will never be ready for it. To Vlahos, Big Change will create Byte City, and the conduct and outcome of wars that occur after Byte City's creation are unknown and fundamentally unknowable.

In "Can Information War Be Deterred?", Stephen Blank reaches similarly pessimistic conclusions about whether conflict can be deterred in the Information Age. Blank even argues that Information Warfare (IW) makes both conventional war and wars employing weapons of mass destruction more likely.

Blank reached this conclusion by exploring the prerequisites for successful deterrence in the context of IW. He argues that four different conditions must be met. First, both sides must have access to relatively similarly understood data about each other's intentions, capabilities, and resolve. Second, both sides must have time to make the right assessment of the data that they have. Third, both sides must appreciate that they each stand to lose something of comparable if not equal value if deterrence fails. Finally, both sides must have the ability to communicate reliably with their systems and each other. Thus, in Blank's words, "for deterrence systems to work effectively, neither side's informational capabilities can be impaired or compromised."

Yet, Blank points out, this is exactly what information warfare in one way or another seeks to do. It may seek to impair access to or reliability of data and information. It compresses time and hides clarity both of sources of attack and reality of attack. And it may seek to degrade or destroy the ability of a command authority to communicate reliably with its subservient systems and components.

These observations drive Blank to a series of conclusions that can not fail to be disconcerting for those who hope deterrence will continue to apply and perhaps even be enhanced in the Information Age. Indeed, Blank's conclusions are disconcerting even for those who hope deterrence might function in the Information Age at the same level that it did during the Industrial Age's Cold War.

First, Blank concludes that IW "is almost by definition counter-command and control warfare." As such, "it strikes at those very relationships and mechanisms that make deterrence possible and effective."

Second, sounding much like Vlahos, Blank argues that no one knows "what the full ramifications of IW strikes on another society" would be because the strikes would not necessarily be "at a tangible, visible, or measurable capability." This, Blank observes, may increase pressure to delegate decisionmaking on the use of weapons of mass destruction to local commanders.

Third, since in an IW scenario a target "can be attacked by anyone from anywhere at any time," pressures for pre-emptive use, especially of weapons of mass destruction and IW capabilities themselves, could increase because potential enemies might believe they are in a “use ‘em or lose ‘em” situation.

Finally, then, Blank concludes that IW may not be deterred, and that it will not make war shorter and more humane. Other forms of warfare will continue and perhaps become even more likely in the Information Age. This, he points out, is no different than it has ever been. Throughout history, Blank says, inventions that at first blush offer a “sunrise of hope” of a world at peace instead yielding “one more false dawn.”

The nest article in the section, Steven Metz’ “Military Strategy and Information Technology: Alternative Visions of Future War,” provides first an overview of the evolving status of the official U.S. Department of Defense vision of future war contained in the Joint Chiefs of Staff’ *Joint Vision 2010* and expanded in works such as *Army Vision 2010*, the Air Force’s *Global Engagement*, and the Navy’s *Forward from the Sea*. Metz sees these efforts as conservative, using new technologies and especially information technologies as force enablers or force multipliers, not as “a locomotive for a revolutionary transformation of the security environment or the nature of warfare.”

Metz uses this observation as his jumping off point to begin his own exploration of what more extreme visions of Information Age warfare may look like. Robots, miniaturization, micro-electro-mechanical systems, organic systems, nanotechnology, and other such revolutionary technologies, most of which incorporate what is currently labeled information technology, are on the near-term horizon and promise to accelerate today's Revolution in Military Affairs in ways that will rapidly outdate the strategies and tactics of *Joint Vision 2010* and its sister documents, Metz posits.

But Metz does not stop with technology. He also explores what he calls "the organizational alternative" and "the environmental alternative" to official strategies and tactics, or put differently, asymmetric challenges. Unlike many other analyses of asymmetric conflict, Metz' analysis does not concentrate on weapons of mass destruction. Rather, he emphasizes enemies organized as networks rather than hierarchies, swarming attacks, non-state enemies, and strategic information warfare, all of which under certain conditions could pose threats to the U.S. and its friends and allies for which they are militarily unprepared. And, Metz points out, the danger exists that responses to the diffuse threats posed by these asymmetric forms of warfare may lead the U.S. to undertake steps to defend itself that themselves become debilitating.

Concluding, Metz observes that information technology is a dual edged sword. It is an immense source of empowerment, but it also brings dependence that can create weaknesses. This, to Metz, is a real danger of current U.S. military thinking about information dominance and dominant battlefield awareness. Metz is even more concerned about the assumption that the U.S. will inevitably continue to enjoy technological superiority. This, he charges, is hubris, especially in the Information Age when technology disperses rapidly.

Metz' ultimate question is "whether the U.S. military can identify and adjust to the changes that information technology is forcing or allowing without a major fiasco." He is much more optimistic than Michael Vlahos. Indeed, Metz even points to the existing futures-oriented programs in the U.S. military as sources of hope. Despite their deficiencies, Metz concludes, "by inculcating the need to think about the future, to think holistically, and to innovate," the U.S. military may be able to react and adapt to the requirements of future warfare once its true essence becomes clear.

"But what are we really talking about, and what can we really do?," William Hoehn asks in the section's final article, "What Revolution in Military Affairs?" "Is the Information Age Revolution in Military Affairs really as advanced as some maintain it is?," he queries. After exploring answers to his first question, he answers the second with a resounding, "No."

Hoehn begins his examination by pointing out that the RMA requires a "seamless melding" of intelligence, surveillance, and reconnaissance technologies; command, control, communications, computing, and information dissemination technologies; and precision force technologies. While acknowledging that the U.S. is far ahead of the rest of the world in these technologies, Hoehn argues that most of the technologies themselves are nowhere near as advanced as they need to be for a true revolution to have occurred, and that no "seamless melding" exists or is foreseeable.

The author presents what he sees as four fundamental flaws in the RMA. First, some of the required components may simply be technologically infeasible. Second, even if all components prove feasible, their integration into a "system of systems" is a technological challenge that far supercedes any accomplishments achieved to date. Third, the RMA has not been subjected to analysis of potential vulnerabilities. Fourth, for mission success, the RMA is dependent on a long chain of sequential events, each of which must be carried out in timely fashion. A brief interruption at even a single point in the chain may lead to system failure, Hoehn points out. So too may massive disruptions of RMA technologies induced, for example, by a nuclear detonation in the atmosphere that disperses a massive high altitude electromagnetic pulse.

After raising questions about the present state and future feasibility of an Information Age RMA, Hoehn turns his attention to the question of what types of military contingencies would benefit the most from an RMA. Hoehn's assessment of the impact of an information induced RMA on large scale maneuver warfare is that absent revolutions in intelligence and senior level decisionmaking, the RMA may reduce the number of troops required, but will probably not eliminate the need to deploy substantial numbers of weapons systems. As for "hostage scenarios" in which an enemy threatens to capture or has already captured a territory of extraordinary value as in Kuwait before *Operation Desert Storm*, Hoehn is skeptical about the utility of the RMA. He also sees the RMA providing little advantage in various forms of asymmetric warfare or in situations of ethnic cleansing.

In short, Hoehn is a true skeptic when it comes to the RMA. Information age technologies may induce change in combat, but to Hoehn, the RMA remains a thing of the future with dubious utility.

CHAPTER 2

GRAND STRATEGY AND INFORMATION WARFARE

By
Daniel Goure

With the publication of Alvin and Heidi Toffler's book, *War and Anti-War*, the world of military thought was rocked by what can only be characterized as a quasi-religious frenzy. According to the Toffler's, societies make war like they make money. In other words, the basic character of economic activity determined the way nations are organized for and conduct most facets of national or group behavior, including warfare. Mankind had moved through three great waves of development from the agrarian age, through the industrial age to the information age. Each of these ages, it was argued, had a characteristic way of warfare. An era in which economic behavior and social organization was increasingly centered on the acquisition, manipulation and communication of information would inevitably lead to information-intensive military operations.[1]

While not the only or even the first argument of its kind, the Toffler's book hit the defense intellectual marketplace at the right time. The Cold War was ending. New technologies were coming to the fore with the promise of transforming our way of life. Economics was becoming global. It was, to borrow a phrase, "the end of history."[2] What better time to adopt a new view of war and warfare.

Military analysts in and out of uniform took up their pens and mounted their rostrums to declare a new vision of the world, society, and war. This great awakening spawned an outpouring of articles on the role of information in warfare and strategy.[3] The term "knowledge warrior" became fashionable for the practitioners of what was variously called cyber war, net and net-centric war, command and control warfare, and information operations. Some proponents of the new age in warfare went much farther than had the Tofflers, writing of a future in which war would no longer be fought with destructive force but rather with the bits and bytes that constituted the building blocks of the new information domain. Proponents of information-only warfare were dismissive of the old fashioned ways of war, from bows and arrows to cruise missiles and nuclear weapons, often referred to as "kinetic" solutions. They asserted that the flow of electrons could be directed almost literally into the mind of an adversary via his data bases and electronic gadgets.

Even more sober-minded assessments often made sweeping generalization regarding the ways in which improved use of information would change the face of future warfare. No less a figure than the former Vice Chairman of the Joint Chiefs of Staff, Admiral William Owens became the prophet of this new vision.[4] It became the centerpiece of the Chairman and the Joint Chiefs of Staff General Shalikashvili's *Joint Vision 2010* that saw a future in which a blanket of information engulfed U.S. forces, enabling them to operate collectively at a variety of distances and against an array of threats.[5]

After a half-decade long orgy of optimism regarding the impact of information on warfare, reality is beginning to set in. On reflection, analysts and practitioners alike are beginning to realize that defining the role of information in warfare is a much more complex task than was originally thought. They are starting to ask some tough questions:

- How does one fight an information war?
- What is the balance between offense and defense in an information-intensive environment?
- What is a usable information advantage, or what good is information superiority?
- How can information actions be integrated or deconflicted with overlapped areas such as electronic warfare, psychological operations, and even that old favorite, “kinetic” warfare?
- How will coalitions and alliances operate when they consist of nations that are striving to exploit the information domain to its fullest and others that are not? Will information intensive nations such as the United States continue to operate with friends and allies?
- Which of many investments in future technologies should be made and in what order?
- What skills will be required for so-called knowledge warriors?

All of these questions are important, but none of them is central. They all require an affirmative answer to the first order question, “Will there be wars in the future?” Anyone looking at events of the last years of the 20th century would be tempted to dismiss this question out of hand. The record of violent military action compiled by the Clinton Administration since it took office, a period of time approximately the same as that since the end of the Cold War, suggests that conflicts involving the armed forces of the United States are likely. But, are we seeing the re-emergence of history or the trailing away of the old order and its habits?

The subject of this essay, grand strategy, is about the pursuit of the supreme national interests of the state. The purpose of grand strategy is to organize the power available to the state in such a way as to ensure national survival, the well being of the people, and the maintenance of national institutions. The Information Revolution clearly has changed the definition of power available to the state. It may also have altered our understanding of what constitutes the well being of the American people and the requirements for the maintenance of national institutions.

Will There Be War?

The overwhelming majority of the literature on information and war focuses on the operational, tactical, or technological levels. It focuses on the contribution of information to battlefield awareness, precision targeting, psychological operations, and the like. The essential premise of virtually all these works is that information is a force multiplier, perhaps ultimately even a force unto itself. The framework in which force will be used remains essentially unchanged from the “pre-information revolution” days. Information is seen as a way of improving the effectiveness of firepower. This treatment of information is in keeping with the penchant in American military thought to exploit overwhelming force. The ends to which this force is directed continue to be those associated with classic warfare.

There is a case to be made that the world, or at least the great post-industrial nations, no longer has the interests or inclinations to engage in major war. The failure of communism in both the Soviet Union and China removed the last great source of ideologically-based antagonisms that could produce major conflicts. The current post-Cold war period also confirmed the centrality of democratic capitalism to a nation’s ability to generate wealth both domestically and through trade with increasingly like-minded states. The absence of ideologically-driven antagonisms, the ability of democratic institutions to manage traditional rivalries and antipathies, and the promise of gain for all reduces the likelihood that nations in the mainstream of the ongoing political, economic, and technological revolution will engage in war with one another.[6] Other observers would add to this explanation a change in the internal character of these democratic and capitalist states, particularly in their demographics, making them less prone to warlike drives.[7] Those that remain unreconstructed politically and economically will, by definition, be unable to avail themselves fully of the advantages of the emerging global order and thus constitute inferior competitors.

There are additional reasons why some question the likelihood of major wars in the future. Classical international relations theory is that war is organized violence conducted by states for political purposes. States are uniquely privileged in this regard because they embody or derive their power from the will of the people. International law legitimizes the use of force by states to protect their territorial sovereignty, people, and other vital national interests.

At one level, it can be said that the Information Revolution in its broadest sense reduces the likelihood of war. The free flow of ideas, people, and foods creates a web of interests and relations that are antithetical to the demands of a state bent on aggression.[8] The availability of information itself can act as a barrier to aggression, denying a state bent on hostilities the ability to concentrate forces and achieve surprise.[9]

The Information Revolution may have an even more profound effect on the nature of war. If war is organized violence committed by states, then any weakening of the power and control of states will naturally effect their ability to engage in war. The idea of the state as the supreme sovereign entity in the international system is being questioned. Some critics of a state-centric model argue that the power of the state must and is being curbed by the growth of international organizations and norms of behavior. Advocates of supra-national visions point to the power of the European Union and the acceptance by most of its members of a common currency as an example of the new organizational paradigm for the international system. Others assert that trans-national forces, such as the globalization of national economies, access to international media, and the growth of information technologies are limiting the power of states and their ability to impose their will on other states, and even within their own borders.

Visionaries assert that the combination of new international organizations and trans-national forces means that the prospects for wars between states will be limited. The rise of the new information economy means that many of the traditional objectives of war, e.g., territory, resources, industrial assets, will be less meaningful. In addition, in a global economy, so it is claimed, destruction of industrial facilities in one country will effect the economy in the aggressor state. As a result, it is argued, states will naturally be constrained in their use of force. Peacekeeping will become the more characteristic use of military power and its use will be sanctioned by international bodies such as the UN or OSCE.

If the likelihood of war is declining, and the severity, scope, and duration of residual conflicts will be limited by virtue of constraints on the resources available to the combatants, it is fair to ask the questions, “What significance does the Information Revolution really have for the future of conflict? How meaningful is a capability to employ overwhelming force and inflict a crushing defeat on an adversary when the circumstances in which such a capability could be exercised are becoming fewer in number?” Information operations may enhance the effectiveness of a given force, just as precision targeting can reduce the number of rounds of ammunition or bombs required to destroy a target. But this is not particularly significant from the perspective of grand strategy.

A more interesting question is not how nations will fight but what they will fight about. The logic of the

Tofflerian position holds that since information is the nascent coin of the realm, nations will fight for control of it. But how is this possible? How does a nation truly gain control over information by force? We can conceive of an effort to capture key installations, equipment, and specialists, much like the race among the allies at the end of World War II to grab German rocket scientists and technology. But that was an unusual situation. Most information is difficult to hoard. Even information that can be hoarded, such as the secret of the atomic bomb, has a short half-life. Typically, valuable secrets are sought through espionage. But it is hard to envision nations going to war to seize or control information, or the people and installation that create it.

If nations will not, or to put it more accurately, will be unable to fight for information, then what will be the sources of conflict in this information-driven world? Some envision a struggle emerging between the secular, capitalist, technology-oriented nations and peoples and those that have a different political, cultural or social orientation.[10] Sometimes this is also referred to as the haves versus the have nots. The latter, while rejecting the values, methods, and even means employed by the former, would still rely on technologies, including information warfare, in order to defeat their adversary.[11] In principal, this represents a characterization of the classic struggle between civilization and barbarian, between the city and nomads, that is as old as human history. It is almost Jungian in character. For that reason, it needs to be treated cautiously.

The image of a titanic struggle between opposing socio-economic and political forces is not supported by facts. Nor is there compelling evidence to suggest that the nation-state as the central focus of human organization and international activity is losing ground significantly to non-traditional non-state actors. The nation-state remains the most effective means ever devised for effectively organizing, containing, and maintaining/protecting the activities of its people that contribute to their well being and prosperity. The nation-state also possesses enormous resilience, making it unlikely to collapse or suffer catastrophic losses in the face of the limited power that non-state actors can bring to bear. Most importantly for the purposes of this essay, the nation-state still controls the overwhelming preponderance of coercive force. It alone can rely on kinetic weapons in overwhelming numbers to enforce its will.

It is unlikely that nations will spend much effort fighting over territory. One of the virtues of the green revolution, modern production techniques, and a global economy is the ability to produce more with fewer inputs. Information technology makes it easier for states to be part of the global economy. Those that cannot avail themselves of these advantages are unlikely to have the wherewithal to pose a serious military challenge to anyone.

The above discussion of the likelihood of major war still leaves ground open for lesser conflicts of serious note. Many of these conflicts are residual in nature, arising from the aftermath of decolonialization, the collapse of the Soviet Union, and the end of the Cold War. Such conflicts almost inevitably will be limited in purpose and scope, both for the aggressor and for the United States. Small vices will produce small wars. The same may be said of small virtues such as the American instinct for intervening in the traditional ethnic, tribal, and religious disputes of others. This also suggests that future conflicts are likely to be idiosyncratic in character and causation, reflecting peculiarities of local rivalries and opportunities. We are not likely to be confronted by adversaries that provide us with the kind of templates of ideology, military doctrine, and technology competitiveness we found so useful for planning purposes during the Cold War.

The limited nature of these future conflicts likely means that their character will be constrained. Not all means can be employed. We saw evidence of this in Iraq and Kosovo. The limited nature of U.S./coalition objectives also produced a desire to limit human and material costs. This resulted, in turn, in an emphasis on limited operations, graduated escalation, and overall casualty avoidance. Cold War military theorists would argue that this reflects a desire to ensure that the gains, largely fixed by pre-conflict statements and policies, outweigh the costs, which are variable in any conflict.

Even the terms employed by the Department of Defense to characterize the largest conflicts included in its planning, Major Regional Conflict (MRC) or Major Theater War (MTW), are by historic and Cold War standards rather small. If such a war were to occur, the general belief among the analytic community is that it would have the following characteristics:

- It would have a regional focus;
- It would be fought by the United States in a coalition with other, like-minded, states;
- It would not seek the total defeat of the adversary but rather the reversal of aggression;

- It would confront a regional-level adversary who would deploy the means of modern warfare—tanks, aircraft, air defense, C3, etc.; and
- Given the proliferation of technology, the U.S. homeland, deployed forces, and coalition forces might also be threatened by specialized capabilities or weapons—space-based support for communications, targeting and navigating, or WMD and ballistic missiles, information warfare, etc.

To the extent that U.S. military capabilities remain equal or superior to that of regional powers—to include Russia—then, all else being equal, we can remain confident in the ability of U.S. forces to achieve their missions. However, we must take into account the fact that the base of U.S. military power is shifting from its forward, and permanently deployed positions of the past to the continental United States. In addition, there is the desire to reallocate the burdens of regional defense, placing more weight, particularly for smaller contingencies, on U.S. allies. The political significance of the change is related to the determination of the administration to encourage allies to become more self-reliant in security affairs. This means, in turn, greater U.S. reliance on these allies when U.S. interests are threatened. This raises, in turn, questions about the capability of U.S. allies to shoulder a greater percentage of the regional security burden and the willingness of the United States to assist them in improving their military and technological might.

The new U.S. approach to exercising military power through the projection of force from CONUS into distant theaters also provides an opportunity for adversaries to adopt a grand strategy of their own intended to complicate U.S. power projection into their region. The acquisition of long-rang ballistic missiles and WMD seems particularly suited to this purpose. In situations where vital U.S. interests are not threatened directly, the adversary may hope to deter U.S. intervention by threatening first-use of WMD either against power projection forces themselves or against the U.S. homeland. The objective is not to defeat the United States militarily, something that no potential adversary will be able to do in the near future, but to undermine the political and strategic connection between the United States and its overseas allies, friends, and interests.

For the United States, the essential grand strategic problem is that of regionalization. Even as the world becomes more interconnected in the infosphere and as economies globalize, states and regions are turning inward politically. While no nation other than the United States has the military, political, and economic capabilities and resources to be a world-spanning power, many see themselves as having the ability to be the dominant force in their own region. Moreover, the trend to region-wide political integration appears to be accelerating. The decision by the European Union at Cologne to make real the promise of a European security and defense identity and to pursue an independent military capability is a sign of this trend.

Due to the range of its interests and the degree of its power, the United States reluctantly finds itself required to act as a world power, and even the world's sole superpower. This does not mean that the United States is interesting in forcing others to conform to its way of life. Rather, it means that the United States must stand for the maintenance of basic order and the free association of nations. At present, there is little to challenge the ability of most states to live as they chose and interact as they see fit. For the United States, as one analyst put it, the job amounts to "policing utopia."[12] Put another way, it is that of maintaining a virtual global presence while husbanding increasingly scarce resources at home.

For the United States to have the political influence it requires in regions of interest, it must contribute to the security of its partners. It can best do so by having the ability to intervene on their behalf quickly and effectively. It also can enhance regional security by serving as a security magnet. To this end, the United States must have intelligence capabilities that can provide strategic warning, the means to project decisive power around the world, and the capability to protect itself, its forces in the field, and the homelands of others from attack.

The problem for U.S. grand strategy is to ensure that it retains access to regions of interest both politically and economically even as new power centers emerge and those regions pursue their own interests. Simply put, the United States needs to retain its relationships with friends and allies and protect U.S. interests with the minimum expenditure of energy and resources, and to do so from a distance. In order to retain its access and presence, the United States must make itself the ally of choice in those regions. It can do so by providing the kind of military capabilities that local allies cannot provide for themselves such as dominant battlespace awareness. It can also provide the capability to balance regional rivalries and prevent the rise of regional hegemons. Finally, the United States can provide regional parties with the strategic depth that most of them lack.

Here is where strategy and the Information Revolution intersect. The Information Revolution provides the United States with an ability to bestride the world, culturally, economically, and militarily, without the requirement for continual forward deployments. The Information Revolution provides means whereby the United States can enhance its value as a friend and ally, increase its ability to project power abroad rapidly and decisively, shield itself and others from attack, and enhance the web of relations among peoples. It is a source of enormous potential power.

In addition, the United States is likely to find itself the guarantor of the freedom of all the lines of global communication and commerce, including those that constitute the infosphere. Freedom of the seas has been a long standing principle of U.S. foreign policy and national security strategy. Freedom of the infosphere may come to be an equally important one. This does not mean freedom with respect to content, but free and continual access, unbroken communication, at least at the nation-state level. This access is important for the maintenance of the global economy and for U.S. access to regions of interest. It is also important as a means of ensuring connection to close friends and allies. Finally, access to the infosphere can be a tool for the promotion of U.S. interests and even, in some instances, democratic values.

Information and Strategy

Most of the credible discussions of the changing role of information in national security focus on ways of improving on the old paradigm. Information superiority, it is argued, provides ways of replacing mass with precision. There has been a lively discourse inside and outside the military establishment concerning the changing character of conflict, a potential military-technical revolution, innovative force employment concepts, and the promise of new technologies rending old weapons and modes of warfare obsolete. Despite this, the Department of Defense and military services remain largely wedded to old military strategies, operational concepts, and modernization plans, including those that proved successful in the Gulf War. While many organizational and operational innovations have been pursued in the past several decades—AirLand battle, for example—we continue largely to operate with concepts, structures, and even plans that at their core are based on the realities of the past.

The strategic and operational concepts designed for Cold War challenges must be thoroughly reexamined in the context of the changed strategic environment and opportunities for further constructive innovation. Cold War conceptions of strategic and theater level operations, deep battle, and centers of gravity need to be redefined to fit future adversaries of various size, strategic position, military capabilities, and regime disposition. U.S. military strategy and operational concepts should be carefully tailored to balance the scope of military operations against the military forces and the infrastructure of the adversary.

Where Cold War concepts were modified in the Gulf War or thereafter we must ask the question whether they are relevant to the conflicts of the future. The services have begun to develop the broad outline of new approaches to warfare. The Navy’s “From the Sea,” and the Air Force’s “Global Power, Global

Reach" have begun the process of rethinking approaches to warfare in the future. But these are only the beginning. Still to be addressed are the critical questions of military doctrine, strategy, operational art, and the organization of deployed forces for combat in a new age.

Central to the reformulation of U.S. military strategy and warfighting concepts is a determination of the decisive point of leverage in future conflicts. The Napoleonic revolution transformed war from a contest between monarchs to a contest between nations. Napoleon's battles signaled the transition point between the two forms of warfare as he sought the decisive defeat of his adversaries by the annihilation of their armies. Napoleon's aims were stymied because opposing nations were repeatedly able to marshal resources of the state and reconstitute their armies to challenge him another day. Inevitably, the aim of warfare became the ultimate subjugation of the opposing nation. This age of warfare culminated in World War II and may only have been ended by the nuclear weapons.

Current conventional military strategy is rooted in these Euro-centric total war concepts. A conflict in Europe was always viewed as a contest between nations, fought with the total resources at each nation's disposal and carried to the enemy throughout its depth to include any elements of the state—energy supplies, internal communications, and manufacturing—considered relevant to continued prosecution of the war. Only by attacking the adversary thoroughly could a nation at arms be defeated.

As a result, the military services of the United States came to define their warfighting doctrines according to roles they intended to play in bringing the opposing nation—the Soviet Union—to its knees. The Army would focus on large land forces to defend Europe; the Air Force would dominate the skies with flocks of fighters and attack the enemy's heartland with a strategic air campaign; and the Navy would clear the seas and carry out its own deep attacks. Army doctrine evolved over the years from a strategy of forward defense to active defense to an AirLand battle that could carry the fight to the enemy by attacking his forces in depth. Army doctrine became focused on preparing the battlefield and maneuvering large land forces to decisive engagements. Air Force doctrine concentrated on clearing the skies of opposing aircraft to pave the way for strikes deep into the enemy's strategic center. Accordingly, Air Force doctrine became focused on identifying critical strategic targets that once destroyed would end the enemy's ability to prosecute the war. The Navy's doctrine was similar with respect to clearing the seas and then carrying the battle to the enemy's strategic flanks and rear.

These warfighting priorities and concepts need to be reexamined in the context of the probable nature of future adversaries. The previous adversary was a highly developed state with a robust infrastructure and vast resources, the pinnacle of development of a military state. Cold War military strategy and doctrine correctly identified the center of gravity of a war effort against such a state as the state itself. But that opponent no longer exists, and a fight for ultimate survival is no longer envisioned. U.S. military strategy is changing to fit a vision of the United States entering a conflict to repel or reverse aggression by a regional actor that threatens an ally or vital U.S. interest. Although occupation of the adversary cannot be ruled out as a future U.S. war aim, it is much more likely that the defeat of an adversary's fielded forces to a point that ensures a very low likelihood of further aggression will be the extent of U.S. objectives.

Given the material, technological, and qualitative advantages U.S. forces expect to possess relative to regional adversaries, these total war warfighting doctrines may no longer be relevant. Moreover, in light of the changes in global politics over the past several years and further changes we can anticipate, they may not be appropriate. Despite incremental improvements in military capabilities, future regional adversaries are generally characterized by low levels of development, weak infrastructures, centralized government control, and extreme regime rigidity. The power of such a state is often embodied in its armed forces, particularly its army. At the same time, most future regional adversaries have little hope of matching U.S. military power, even if they are fortunate enough to acquire an arsenal of Western weapons systems.[13] If the army is the regime's center of gravity, then warfighting doctrines designed to attack the nation-state at its core may no longer be necessary and may even be counterproductive. How, then, should U.S. warfighting doctrine and operational concepts change to fit the new strategic environment, U.S. military strategy, and military-technical opportunities?

In addition, given the reductions in U.S. military forces, it will be critical that the limited U.S. forces fielded against such a regional adversary are focused on the proper center of gravity. U.S. military forces will not likely have the latitude of purpose or the luxury of resources to overwhelm the adversary by attacking an entire range of targets in search of the center(s) of gravity. The restructuring and redesign of the armed forces will likely require a different set of modernization priorities from the plans laid during the Cold War. But unless innovative, sound, and balanced operational concepts are formulated to guide these changes, the services can be expected to guard and champion the familiar and prized weapons programs of the past.

Military planners are going to be confronted with a number of serious issues as they try to reconcile warfighting requirements to the changes in regional conflict scenarios, to the political realities of the new millenium, and to declining resources. Will the reduction in U.S. military forces demand that U.S. military strategy and war fighting doctrines be weighted in favor of one particular form of military power, i.e., air power, land power, naval power, strategic deterrence? Will the military strategy call for creating one form of military power as the primary instrument while preserving secondary forms for application to other aspects of the strategy or unique war fighting environments, i.e. air power as the spearhead of most operations, land power as a holding force, and naval power for power projection in remote and austere environments?

The answer is that warfare is changing for reasons that have little to do with changes in technology, including the Information Revolution. It is increasingly apparent that for the United States and its principal allies the purposes of war, and hence the kind of military strategy to be employed in them, is changing for political reasons. U.S. military doctrine is placing greater emphasis on a high intensity of combat, from the beginning and throughout the war, striking targets from the front to the rear, including an enemy's leadership, for the purpose of breaking his will to wage war. The objective is to end the war, not to achieve a set of objectives classically defined. The emphasis will no longer be placed on the conduct of war as a series of battles, comprising a self-contained operation, with the ultimate aim of defeating the enemy through the destruction of his forces and if necessary the occupation of his territories and the overthrow of his government.

The need for swift war termination is conditioned by the increased vulnerability of the U.S. homeland to small regional adversaries. As its exists today, not fully exploiting the potential of advanced technology, the U.S. military is capable of defeating any prospective regional opponent. Together with traditional regional allies, it is almost unassailable. Hence, potential adversaries appear to be pursuing the acquisition of weapons of mass destruction and long-range delivery systems. The ability to hold the U.S. homeland or the territory of U.S. allies at risk may deter U.S. intervention or limit our ability to deploy force decisively and early in a conflict.

For the United States, the new reality of war will place tremendous emphasis on the battle for first salvo. As demonstrated in *Operation Desert Storm* and *Operation Allied Force*, powerful initial air and missile strikes can so disrupt and paralyze an adversaries defensive capabilities as to almost literally determine the course and outcome of the conflict. In order to achieve early dominance and the advantage of the first salvo, there will be an increasing need for surprise, both tactical and strategic.

Not only must the United States win the engagement early, but it must do so under relatively severe political and operational constraints. The critical lesson of Kosovo is that modern coalitions fighting limited wars are inherently hampered by their reluctance to use the force available to them. Hence, there is the inevitable vital search for an adversary's centers of gravity, those structures, assets and institutions that if threatened with destruction or actually attacked will force the adversary to cease his aggression or even capitulate.[14]

Winning early and decisively will require superior intelligence and battlefield knowledge. Too often, the focus of information revolution discussions has been on the operational and tactical requirements for awareness. Relatively less attention has been devoted to the increased requirements for strategic intelligence. Granted that this is a more difficult requirement to meet than precision navigation or targeting, strategic information is likely to be even more critical to the United States in the future. Knowing the intentions of potential regional adversaries, the status of their WMD programs, and the state of their military establishments will be critical to U.S. grand strategy.

The United States is investing relatively little in the way of new technology or methods at the level of strategic intelligence. New generations of satellites are going up. Increasingly, the assets of the intelligence community are being exploited for operational and tactical purposes. In contrast, the effort to exploit open source information, to mine the Internet, and to improve human intelligence is lagging. It is ironic that at a time when the sources and forms of information are proliferating at an increasing rate, the intelligence community remains wedded to its ability to "see" things.

In general, there has been a misplaced focus on sensing and the accumulation of data in the development of information warfare capabilities whether by the intelligence community or by the military. It is processing and the acquisition of knowledge that is important as distinct from the accumulation of data. We already see a lot, maybe even enough. We often do not know what to make of what we see. Even if we recognize what we are seeing, the capacity to act may be restricted. It is the apparent desire by some military experts to make the soldier of the future the military equivalent of a day trader, able to surf the military infonet and make instantaneous responses to small changes in the situation. Information mania is leading to the weighing down of soldiers with so many electronic gadgets that they cannot engage in close combat. Information warriors resemble knights of the late fifteenth century. Then, warriors were so encumbered by encasing armor designed to permit them to survive on the battlefield that they had to be winched into their saddles and could not rise once unhorsed.

Moreover, the practitioners of information warfare are overly confident in their ability to acquire data. There is a war underway between seeing and denying sight. The effort to deny information is at least as old as that of discovering it. Moreover, many U.S. adversaries have become increasingly adept at the arts of cover, concealment, and deception (CCD). They know our methods and technologies and are discovering ways to counter them. We know that a number of states have been successful at concealing their strategic activities from our best sensing systems. The proliferation of encryption programs and untappable communications systems will further complicate the intelligence collection problem. Thus, the idea that the United States lead in the Information Revolution means that it can readily win the battle for intelligence is unlikely to hold true.

The recent conflict in Kosovo holds important lessons about how far we have come in exploiting the Information Revolution and how far we have yet to go. Kosovo may be be the first Information Conflict. It certainly was the first all-precision air war. We have solved most of the problems associated with navigating aircraft to their targets and placing bombs on the desired location.

At the same time, there is growing evidence that the Yugoslav effort at CCD was successful. Relatively little damage was done to the forces occupying Kosovo.[15] Estimates of the number of tanks destroyed by NATO air attacks were off by almost an order of magnitude. Yugoslav forces employed a number of CCD measures, including dispersal, use of buried and hardened structures, and the employment of decoys to successfully deny NATO's ability to fully exploit its command of the air. The destruction of fixed targets was relatively easy, at least initially. The ability to target mobile field forces proved much more difficult. This was true in large measure because field forces could act on their own initiative, thereby changing the "information" on which targeting was based.

Beyond the evident difficulty of acquiring information dominance over a thinking, agile adversary, there is the equally serious problem for the United States posed by adversaries' efforts to deny the United States access to their theater or region. Anti-access strategies rely not on classic conventional warfare capabilities but on special weapons and tactics, so-called asymmetric techniques, to threaten U.S. power projection capabilities and strategy. Submarines, cruise missiles, mines, ballistic missiles, and information operations are all tools of asymmetric strategy. These capabilities are not in themselves means for winning a war. Rather, they are the means by which an adversary can either deter U.S. intervention or, at a minimum, complicate and delay the projection process. Future regional conflicts may well become a matter of an anti-access strategy versus one based on distant warfare.

A combination of anti-access and CCD may be the best way to thwart a U.S. military strategy based on a combination of power projection and information superiority. Anticipating a regional conflict, the United States will seek to identify and target the adversary's anti-access capabilities. The adversary will attempt to hide and protect those systems. As NATO discovered in its efforts to achieve air superiority over Yugoslavia, the mere survival of the adversary's air defense systems meant that air operations had to be conducted in a different manner than if those defenses had been destroyed at the outset of the war. Yugoslav air defenses exacted a price in virtual attrition of NATO air assets. The inability to find even a small number of anti-access systems such as a long-range ballistic missile armed with WMD could be sufficient to deter the United States.

One form of anti-access warfare that should be of particular concern to the United States is an attack in space. It is common knowledge that the United States is increasingly dependent on space-based assets for its global economic activities as well as for the operation of its military. Rather than threatening the U.S. homeland, an adversary could use a nuclear-armed ballistic missile to threaten U.S. and international assets in space. It is estimated that some 1,500 satellites will be deployed in the next decade. At an average cost of $100 million per satellite, this is an asset base of some $150 billion dollars. In addition, the world's commerce travels through satellite links. The threat to the global economy from such an attack could be a significant deterrent to the United States in a regional conflict. The possibility of such a threat leads naturally to the question of the requirement to defend space and to control access to space.

Much has been written about the use of the Internet by adversaries as an avenue of attack on the U.S. homeland.[16] In response, the U.S. military has devoted enormous effort to the conduct of defensive information operations. Relatively less attention has been devoted to what is an equally important subject, U.S. offensive information operations. During the Kosovo conflict, there were press reports to the effect that U.S. computer experts were attempting to use electronic means to seize funds deposited by Yugoslav President Slobodan Milosevic in foreign banks. It is here that the Tofflerian logic that the means of warfare follow the means of production may be proven correct. As the dominant information power, the United States for the present may be in the best position to dominate the realm of information warfare.

As hackers and counter-hackers line up on opposite sides of the Internet, there is a growing prospect for major conflict in cyberspace. Indeed, the idea of warfare in cyberspace has moved from the pages of science fiction to that of mainstream military writings. Yet, this environment is like no other in warfare. It is artificial. We know what damage can be done to the physical world as the result of war. What could be the consequences of conducting war on the Internet? Can you fight in the infosphere and not destroy it? Can the Internet be so polluted by the electronic equivalent of germ warfare that it becomes unusable? This harkens back to the late 1980s debates about the possibility that a U.S.-Soviet nuclear exchange could produce a nuclear winter.

As suggested above, U.S. grand strategy is likely to be closely linked to the growth of the infosphere. It may be in the U.S. interest to see that domain protected, even at the price of abjuring its use by our military for offensive purposes. It could be in the U.S. interest to seek a cyberspace equivalent of the Environmental Modification Treaty (ENMOD). The ENMOD Treaty prohibits military activities intended to alter the Earth's ecosphere. An outright ban on offensive information operations, on the lines of the ban on the use of chemical and biological weapons, might be even more to the point. We need to consider what a military campaign of information operations in cyberspace will involve and the degree to which the interaction of offensive and defensive actions might cause damage to the cyber environment.

Finally, it is only a small step to suggest that banning offensive information operations could lead to a desire to prohibit infosphere pollution. There is great concern among Internet users about the problem of "spamming." As more commerce and communications moves to cyberspace, maintaining the flow of data may become a crucial economic and political security problem. It may require force to ensure freedom of cyberspace much as force was required to ensure freedom of the seas and protect sea-based commerce. It may be more important to create a cyberspace police force than to improve our capability to use information for military purposes.

New Concepts

How should the United States proceed in mapping an investment strategy for information capabilities in keeping with its emerging grand strategy? In a time of uncertainty and change, what is required is not absolute fidelity with respect to small events or specific targets, but a broad understanding of trends, changes in behavior, and intentions. To this end, the United States needs to develop means to turn data not just into awareness or even knowledge, but into understanding. We already collect enormous amounts of data. Simply accessing open source materials properly will multiply the data flow to the U.S. national security apparatus many-fold. Yet, it is not clear that we have the means, technical and operational, to make the data useful.

To first order, the problem is straightforward, but not simple. To paraphrase a phrase, “It’s the software, stupid.” The current emphasis in intelligence collection on gathering data and developing more sophisticated machines and architectures for data collection needs to be reigned in. More effort must be placed on developing software to sift data, compare and contrast information from different sources, and provide timely data fusion. For example, automating the target designation and checking process in the air war over

Yugoslavia could have prevented the bombing of the Chinese Embassy.

Kosovo also demonstrates that while the United States and its allies have the technical means to locate and strike virtually any fixed target, and even many mobile ones, they lack the ability to relate an air campaign to desired outcomes on the ground except at the most obvious level. Despite the Alliance's information superiority, it was caught by surprise by the strength of Belgrade's resistance and its apparent willingness to take losses. Moreover, while NATO could find and strike a range of targets, it could not define with any precision the impact of target set destruction on the will of the adversary. Thus, while we could measure degradation in functions and capacities on a sectoral level, we could not relate that information to the overall strategic purposes of the conflict.

While the United States clearly desires adequate information with which to conduct classic military operations, the longer-term goal should be to develop the means by which to gather and process enough information so as to be able to understand and manipulate macro-level phenomena: e.g., weather, group psychology, economics. The effort to map the human genome is leading to major biomedical discoveries that quite literally may banish death. Each of these other areas will require very different data collection architectures, software packages, and reporting systems.

There is a tendency in modern information operations to see the process of data collection as essentially passive. Yet, if information is likely to be as important to warfare in the future as many suggest, then part of military doctrine and strategy should be the effort to create the necessary information. The U.S. military should be in the business of making information, not merely collecting it. To this end, military planners need to consider how to conduct information-creating operations. A current example is the use of decoys and drones to draw out an adversaries air defense weapons, thereby pinpointing them for destruction. Attacks on landline communications that force an enemy to rely on radios with the attendant opportunity to intercept communications is another example. Larger information-collection operations would be designed to cause dug-in enemy forces to move, thereby making them visible and more easily targetable.

The battle for information superiority will inevitably lead to the development of more advanced counter-information capabilities. The same information gathering capabilities necessary for offensive operations can also be used to perfect CCD measures. The production of stealthy aircraft includes the use of detection systems to test for any undesirable emissions. As information technology proliferates, opponents will learn both how good the United States is at information warfare and how to improve their own countermeasures.

Information assurance for the U.S. homeland is the ultimate in civil defense. It must rely predominantly on actions by individuals, corporations, and institutions to protect themselves from attack. This suggests that defensive information warfare should be the domain of civilian agencies including law enforcement, while attack warning, attack assessment, and offensive operations are the realm of the military.

At the level of grand strategy, the United States must shift from the Cold War strategy of protecting its technological superiority through restricting its dissemination and proliferation to a strategy of staying ahead of an opponent. A vibrant, growing infosphere is fundamentally in U.S. economic and security interests. Moreover, the United States runs the risk that if it too carefully husbands its information technology lead, it will find itself alone, unable to operate with other nations in coalitions. Maintaining alliances and overseas relationships and being the ally of choice in regions where vital U.S. interests exist means being able to plug into the military and civilian networks of those states. To do this, we must share technology and know-how. Naturally, some critical capabilities and technologies need to be protected, but far fewer than are currently restricted. A new export control policy needs to be developed in the information technologies area, one which focuses more on the advantages of ever-widening networks.

[1] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-First Century* (Boston: Little, Brown and Co., 1993).

[2] For an updating of his original thesis see Francis Fukuyama, "Second Thoughts," *The National Interest*, (Summer 1999), pp. 16-33.

[3] See for example: Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (New York, NY: Thunder's Mouth Press, 1994); John Arqilla and David Ronfeldt, "Cyberwar is Coming," *Strategic Review*, (Summer 1995), pp,. 141-165; John Arqilla and David Ronfeldt, *In Athena's Camp: Information, Power and Grand Strategy* (Santa Monica, CA: RAND, 1997); Martin Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, (Washington, DC: National Defense University Press, 1994); Richard Szafranski, "Toward a Theory of Neocortical Warfare," *Military Review*, (November 1994); C. Edward Peatree, Kenneth Allard, and Carl O'Berry, "Information Superiority," in Daniel Goure and Christopher Szara. Eds., *Air and Space Power in the New Millenium*, (Washington, DC: Center for Strategic and International Studies, 1997), pp. 117-131, 1997.

[4] William Owens (USN, ret.), "The Emerging System of Systems," *Military Review*, (May-June 1995), pp. 15-19; William Owens and Joseph Nye, "America's Information Edge," *Foreign Affairs*, (March-April 1996), pp. 20-36.

[5] General John Shalikashvili, USA, Chairman, Joint Chiefs of Staff, *Joint Vision 2010*, (Washington, DC: U.S. Government Printing Office, 1995).

[6] See Francis Fukuyama, "Second Thought," op.cit. See also, Michael Mandelbaum, "Is Major War Obsolete," *Survival*, (Winter 1998-99), and Mandelbaum's exchange with three noted strategists in *Survival*, (Summer 1999).

[7] Edward Luttwak, "The Crisis of Classic Military Power and the Possible Remedy of 'Post-Heroic' Information-Based Warfare," in Ryan Henry and C. Edward Peartree, eds. *The Information Revolution and International Security*, (Washington, DC: Center for Strategic and International Studies, 1998), pp. 70-104. See also, Martin Van Creveld, *The Transformation of War*, (New York, NY: The Free Press, 1991).

[8] David Gompert, "National Security in the Information Age," *Naval War College Review*, (Autumn 1998), pp. 22-41. See also Lt. Colonel William R. Fast, *Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age*, (Washington, DC: Institute for National Strategic Studies, 1999).

[9] Martin Libicki, "The Emerging Primacy of Information, *Orbis*, (Spring 1996), pp. 261-276.

[10] William S. Lind, et al., "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, (October 1989); John Arquilla and David Rondfeldt, "Cyberwar and Netwar: New Modes, Old Concepts of Conflict," *RAND Research Review*, (Fall 1995).

[11] Roger C. Molander, et al., "Strategic Information Warfare: A New Face of War," *Parameters*, (Autumn 1996), pp. 81-92.

[12] Andrew J. Bacevich, "Policing Utopia," *The National Interest*, (Summer 1999), pp. 5-15.

[13] Christopher Parker, "New Weapons for Old Problems: Conventional Proliferation and Military Effectiveness in Developing States," *International Security*, (Spring 1999), pp. 119-147

[14] Lieutenant Commander Jeffrey A. Hartley, USN, "Information, Technology, and the Center of Gravity," *Naval War College Review*, (Winter 1997).

[15] Daniel Goure and Jeffrey Lewis, "Erosion of U.S. Military Power: Evidence from Operation Allied Force," unpublished manuscript.

[16] Jams Adams, *The Next World War*, (New York, NY: Simon and Schuster, 1998), pp. 172-191.

CHAPTER 3

THE WAR AFTER BYTE CITY

By
Michael Vlahos

It was the greatest military power of its day.
Always the innovator, its technologies of war were the newest,
Its command and control the best of the best.
Its ability to mobilize national resources was matchless;
Its traditions the envy and admiration of all,
And surely, imitated by all.
It was the world's military superpower, And it owned war.

But now peace was everywhere.
Its great armies, mobilized for decades, were drawn down.
What had been the center of grand strategy, the cockpit—
Central Europe—
Was now a portrait of like-minded states.
So the great nation refocused,
Turning its military toward new roles.
It built a mobile deterrent force:
A rapidly deployable army that could be rushed
To quell a regional contingency (or two!) and restore stability.
It reshaped its military forces

> *Around a core, professional force*
> *That could be used flexibly to achieve the larger, strategic goal.*
> *The preservation of a stable world system.*[1]

Of course, I describe France in 1860.

But there is something familiar there for the United States. Like France then, we are today's *grande nation,* and we have been for some time in this American century. Like France then, American culture has set world fashion, and our English is the world language. We too seem set now in a long peace. Does a passing historical resemblance tell us anything about the future of our own national security, or the future of war itself?

Four decades before, France had been the defeated superpower in 1815. Yet, in the long peace after the wars of Napoleon, France regained military preeminence only briefly lost at Waterloo. By 1860, France again seemed astride the earth like a god of war:

- Who wrote the doctrine of war everyone used? Henri Jomini.

- Who was the innovator? The French developed the first breech-loading rifle—the *chassepot;* the first shell gun—the *paixhans;* the first machine gun—the *mitrailleuse*; the first ironclad battleship—the *Gloire.*

- Whose army had real global reach? With successful offensive and peacekeeping operations just recently concluded in Spain, Italy, Algeria, and the Crimea, the French army would soon sortie even to Mexico.

France in mid-century was a world power, using its military power to balance and manage world order. France was pledged to preserving a world system and nearly 50 years of stability. Like the United States today, France in 1860 was the status quo power in a world in which the status quo, stability, and the old system itself were about to end. And end they would, in a big bang for France.

Ten years later, the *grande nation* began a historical reeling from which it would never recover. War with the German Federation would humiliate the French, destroy their reputation for war forever, and end also their long certainty of national greatness.

France pushed for war, but every military move their *ancien regime* (Louis Napoleon's Second Empire) made ended in embarrassment; piecemeal transport, haphazard mobilization, divided command, and poor intelligence before battle was topped by army lethargy and skittishness in the field. The Germans, in contrast, greased their rail network to concentrate superior forces; they had the French order of battle down cold; and, in the field, everyone knew what to do. Attack, attack, from meeting engagement to meeting engagement, until the French imperial armies were each surrounded, at Sudan and Metz, and so forced not just to surrender, but to pass under the yoke of defeat as public theater. The French even got their high-tech wrong. The *mitrailleuse* may have been a hot piece of equipment, but it had no range. Yet it replaced one-fourth of all French field artillery. France's marvel—a machine gun—gave the Germans fire superiority at long range, and Prussian cannon cleaned up. The passage to defeat stripped the French of part of their very national identity.

Many U.S. military analysts believe that this fate could never happen to them. *Of course not.* Like all analogies, this one is imperfect and, in mixing military metaphors, manipulative even. *Of course.* Still, as different as they are, two times and two peoples and two ways of war, France then and the United States now share the same strategic problem: “Big Change.”

France did not lose in 1871 because it was stupid or unlucky. Certainly, its war technologies and combat experience were superior to Germany’s. France lost in 1871 because a revolution had swept Europe, and that revolution changed war. The French military and the ruling national elites had not kept up. They had missed the revolution in warmaking.

If you could go back to 1860 and tell this to French ruling elites, they would be offended. They would protest: “We have the world’s most modern military machine. Look at our record of innovation: Superior French science and engineering have changed the face of war!” So everyone thought. You could see it in every newspaper-just look at Daumier’s grisly cartoon, “Triumph of the Needle Gun”: New gun, new ship, new war. If you went back and talked about a revolution in war, people would nod their heads: “Yes, there is a revolution: the ironclad revolution at sea, and the breech-loading *rifle-chassepot* and needle gun-on land. Yes. These are revolutionary weapons.” Everyone thought that revolutions in war were about new weapons.

Yet it was not weapons at all, but the Big Change in ordinary life—the life of people in society—that had changed war. The new artifacts of daily life were what brought revolution in war, especially the railroad. The railroad was the tool of Europe's transformation, the agent at the heart of industrial revolution. The railroad had brought whole pastoral worlds to the new cities of brick and iron. The railroad could also bring whole cohorts of young men to the new killing grounds of the needle gun. Between 1815 and 1870, industrial society created industrial war: War by mobilization, war by train timetable. In 1860, that war had not yet been fought; it was still theory in the mind of Moltke*.*[2]

New war had been enabled, but not enacted. France's elites were free for a time yet to pursue old wars with modern cosmetics, wars still won by quick offensive maneuver and long-service veterans, without apprehension that this way of war was already dead. The French were used to fighting their counterparts: the grizzled professional corps of other monarchs—like the Austrians they met at Magenta and Solferino, or the Russians at the Redan—or tough tribesmen in the world outback—like Mexican guerrillas or Algerian Tuaregs. In imperial France, as in Austria, Russia, and Britain, war was not "politics by other means," *but policy* by other means. It was the finely calibrated tool of Europe's top ruling regimes.[3]

And the French elites could still believe the future of war was theirs, as long as they stayed ahead of all others in weapons technology and kept their warrior ethos stoked hot. There were no worries here.

This is the point of comparison. We are in the midst of an economic upheaval equivalent to the industrial revolution in its capacity to transform our lives. Like the industrial revolution, this metamorphosis will reach up to politics and to war and remake them as well. But America's ruling elites have defined a world system that does not allow for the possibility of Big Change. Like the French plutocrats of the 1850s, the old Cold War establishment is pledged to preserve the old paradigm meaning, centrally, itself to be labeled by sociologists as a functioning subculture; or more straightly, as a characteristically sprawling U.S. ruling establishment that, shorn of its entitling Cold War, now wishes to extend the *noblesse oblige* necessary to manage an unruly world—at all costs. It defines the United States as *the status quo power,* its sacred word is *stability,* and its imperative verb is *to manage.*

The military component of this ruling class sees U.S. military power as the ultimate world management tool. War is defined as combat operations in pursuit of stability. Some in the national security subculture talk quietly about a revolution in war, but they describe this revolution as did the French military innovators of the 1850s: a revolution in weapons.

This, then, is my four-point hypothesis:

1. *The world economic revolution is a true Big Change, what old German philosophers would call a phenomenon of world-historical significance.* As it transforms individual societies across the world, it changes the very patterns of relationship between societies: what we call the world system. Thus, economic revolution changes the world system as well as the world's societies. Here, change comes first as systemic breakdown. New norms—perhaps a new system—will evolve later.

2. *Economic revolution will bring upheaval to world cultures as old ways of life are torn apart.* Upheaval will encourage new belief systems, as people seek new meaning out of the shock of Big Change. Change

will hit different peoples in different ways. Culture and environment will shape different demands for new meaning around the world. New bodies of meaning that arise—whether we call these religions or ideologies—will look different, act differently, and, most important, see big differences between each other. New differences will lead to new human conflict.

3. *New war will serve the needs of new meaning.* The new ideologies and religions born of economic revolution will use the new tools of revolution to win. Industrial war used the new tools of railroad and telegraph, assembly line, and spreadsheet to serve the war visions of the new ideologies: mass democracy and its competing *-isms.* New war will be as determined and as opportunistic—and new meaning will have no ties to old war.

4. *The United States, the status quo power, greatest of the old powers, will not only still be fighting old war, but still be thinking old war.* The successful bureaucracies of old war will continue to refight old victories and continue to dress future combat in the cool desert camouflage of far battles long won. The United States will still have the world's best high technology, and our people will have the combat experience and the military professionalism. But our mythic reputation, first built on a good war fought eight or nine decades ago, will be both our glory and our curse, and we will await our Sedan.

Let's look at this hypothesis point by point.

A Time of Upheaval

Of all world cultures, the United States alone holds progress as a sacred, votive object in its ethos. Boosters have fondly called the 1900s a “Century of Progress,” meaning, by implication, that progress is a gradual, incremental thing, accommodating itself to the world it finds, changing it in polite if not always comfortable ways, giving us time to familiarize ourselves with the new. Every wrench has been buffered by its careful insertion into our lives. We did not jump from vaudeville straight to color TV; it took decades.

Yet, this is not a time of progress: It is a time of revolution. Change, instead of stretching the fabric of reality, is about to rip the canvas. But we are not prepared to see revolution for what it is.

Part of our problem is that we have disarmed our own language. In our vision of progress, we have used the word *revolution* as a commonplace. It has been used as an accent, a spicing for product debuts: television was a revolution, the atomic bomb was a revolution; and so was the jet plane, then the video cassette recorder, Dolby sound, and the microwave oven. These were products that amplified and altered our lives, but in no way did any of them fundamentally change our *way of life.*

We have forgotten what revolution is. We are about to be reminded.

The Second Surprise: It Is Our Own Doing

The Big Change is not happening *out there.* We are making it happen *right here;* we are bringing discontinuous change to ourselves.

The United States, the premier status quo power, is now that very status quo’s undoing. We are the dynamic force actively dismantling the old paradigm, the old world system. We are the system breaker. We are the makers of revolution, like Britain's self-made industrial revolution of the last century. We are bringing the new railroad to American life, and, like the railroad, our invention, what some call the Internet, will transform first our lives, and then the life of the world. As the railroad created a new network of cities and an urban, industrial society, so this new network that we are laying will replace the urban, industrial world with a new city, a new gathering place for American life: Byte City *(Industrial speak* still tries to call this place "The Infosphere" or, in its most arcane form, the "global information infrastructure").

Yet it will be so much more than this. Like all revolutions in life, this one is hard to describe before the fact. It is easier to ask the question:

What Does Byte City Mean?

For U.S. business, and the American way of life, it means the following:

1. *There will be no distance—as well as no time—to transactions. This is happening now.* Business happens when you want it to happen. Our TV ads scream out the possibilities. Today, money moves in an instant everywhere (talk about velocity!), but this is at the trading level. Think of each of us being able to buy and sell, move money around, pay bills, do all things economic, wherever we are, at all times of day. But in the year since this essay was first written, all this has become commonplace. What is not yet common, or even legal, is real security. The breakthrough that must happen before the world's business migrates to Byte City is the very thing that threatens old nation-state authority:

unregulated encryption. But it will happen, because we want it to happen.

2. *There will be no distance or time barriers to meeting and working in Byte City. You will be able to meet anyone, anywhere, anytime, with the fidelity of digitized life. It will not be videoconferencing, and it will not require headgear*. Now this development is still in the 5-10-year realm. Try to imagine, 10 years from today, working in a place that is not real but feels real. It is a place where you can find anything (well, almost anything), and meet anyone (well, consent is still needed). And when I say meet, I mean meet, as in a social setting relaxed enough to reasonably substitute for face-to-face and in-the-flesh. Could I describe this new place in graphic, pixel-by-rasterized-pixel detail? Of course; but of course, I would surely get those details wrong. What holds back even straight-line techno-imagination for us is not our timidity, but simply that we are too deep into the richness of our own present. To us, technology expectation is something we can buy next Christmas: talk about high-definition television (HDTV), or a 500 MHZ Macintosh! I'm talking 10 Christmases from now, an order of magnitude from now. Raw processing power has doubled about every year for the past 50.[4] Most believe that trajectory will last for at least another 10. Just enough, maybe, for Byte City.

3. *There will be a new standard of value, defined by the marketplace. People will set value for knowledge, directly, person-to-person.* Think about living and working in the rich ether of this new place. Think about how you can find what you want, get to look at (if not buy!) what you want, meet just about anyone you want to work for, or get work from. People who do good work

will have every advantage in this world, and people who don't, won't last long. The marketplace of Byte City will not only be history's grandest bourse, but its fairest, and toughest, as well. Right now you can post your resume on the Internet: like ancient script from another age, the assembly-line age. Resumes were cultural code, designed to let potential employers know you fit the mold. But in Byte City, we can go out and find others self-tailored for the work we want done. How? Wait for the rapid rise of Byte City's most pervasive service job: the agent. Like Charles Dickens's clerks with starched four-inch collars, these will be the finders that keep the new economy flowing and as their ubiquitous tool of trade, look for artificial intelligence (AI)-mutating, object-oriented, semisentient databasing extensions, instead of quill pens.

4. *The pressure for openness and transparency of transaction will be absolute.* There is a new book out in the mall chainstores: *How to Look Good on the Net.* Right now, we know the World Wide Web as a kind of high fashion place—it is the place to show off, to strut. As in any revolution, fashion will conspire with the art of the possible to encourage new forms of human display. Byte City will pronounce bazaar in many ways. But the insistent power of Byte City as global marketplace will demand performance. People together are demand. When most people's livelihoods rely on Byte City, the new society of Byte City will, as all new societies do after early, feckless, experimentation, demand truth—truth through voluntary validation. The transparency of this new human place, and the requirement of truth for business trust, will elevate our ethos.[5] People will get further by being truthful, and the rewards for being open will

overwhelm the risks in scamming and deceit. This implies a very different human environment than that of late industrial civilization. That world, though it came to call itself democratic, actually encouraged a kind of human tyranny built into its very social architecture. A world of tightly refined, top-down hierarchies specialized in controlling information; and information-control equaled people-control.

Byte City will break this all down. But remember, Byte City is just a metaphor, a material hook for a big change wholly immaterial. This is why we must try not to think of this revolution as “neat new stuff” (an “information revolution”), or even as a transformation of life (a “third wave”), but as new reality: *a new human design.*

But what is “a new human design?” It sounds pretentious; but our response, really, is less scorn for the two-dollar words than it is a fear of the phrase’s very remoteness. We cannot, at the end of an age, imagine what it really means to enter a new human place. Whatever that place is does not matter. We can argue over the artifacts of what will be until its coming ends all argument. But *what* doesn’t matter. All the *whats of* Big Change—all the fancy high tech in all of its splendiferous baroque detail—do not matter, except as the agency remaking us. It is *us* that matters. And it is *us* changing, forever losing touch with the familiar landscape of our lives today—this is what we fear, this is what we do not want to imagine. Not until we have to.

That is how we can know we are still in the very beginning of our revolutionary times. Like Britain in 1815, just coming out of its long war with an evil French Empire, we are the world’s triumphant people, and, at last, we are in full control. If we could go back and ask one of Britain's winners—maybe a country squire—to imagine his home as a networked world of industrial cities, with its people huddled in brick slums, talking democracy while slowly stripping electoral power from its landed class…well, he would be horrified.

But in something less than a century, starting in the 1790s, Britain remade itself. And what stands out most about their Big Change is less the railroads and the cities and the mills than it is the contrast in the way people thought, before and after. A world that had gone from chattel slavery as big business to women openly demanding the vote is a world that has transformed the meaning of what it is to be human. The corruption, licentiousness, and abuse of all authority that were celebrated at the start of the 19th century, had been criminalized by its end. A new *zeitgeist* rode the rails, along with the new social networking that George Stephenson's infernal invention, the locomotive, had wrought.

Britain's example should remind us why calling our new world an "Infosphere" is misleading, just as it is to think of our Big Change as an "Information Revolution." Yes, information is the building block of this new world, and information has material power with us, just as much as mechanical things of steam and iron once did. But the predominant factor in human reality is what people do in this new place; or more precisely, what new definition of themselves they choose to fit this new place.

It is easier to imagine how this could happen if you call the new place something suggestive of a new human design. Hence the moniker Byte City. Though we will come to live in an info-landscape, contoured by our infinite sculpting of bits and bytes, we will shape it into a familiar social den: forum, piazza, boulevard, main street, neighborhood, casbah. Human designs are always tied to the touch and smell of their places. So to arrive at the new human design, it helps to think of it as a true place: where we play, work, live…and, probably, fight. Once we build it, it will let us change with it. Because like the first cities—like Jericho and Ur—and then the imperial metropoli that followed—like Rome and Constantinople, Baghdad and Beijing—Byte City will be the *terminus.* It will be the place where all information goes, so it will be for us like what Rome must have been: the place where all roads end.

So, if you can, permit the thought of something totally new. Then it will be easier to talk about what happens to old things, when the new hits.

There will be a new economy, built on knowledge services. There will be an explosion of productivity and a whole new workforce. Work will take on wholly new patterns: Commuting will die, for example. It will be a new way of life for most Americans. There will also be an end to the old workforce, and to the old job ways, the old rhythms of life built around manufacturing and the servicing of the machine. This change will mean dislocation, anxiety, fear of the future. It is happening right now, but it will get much worse. Many will do very well in this new world, as they are doing right now.

But many will not.

We are in the beginning of an upheaval the likes of which we have never known. Nor have our parents, nor theirs, nor theirs.

It means this for U.S. politics: The last Big Change overthrew not just regular people's way of life, but how all life was organized, how whole countries were ruled. As millions of Americans find themselves in the fearful, rollicking slide of Big Change, stripped of old meaning, they will demand new meaning: What is my status in society? How do I belong? What is my worth? What kind of life can I expect for my family, what kind of future for my children?

These questions, when asked collectively, will tear apart U.S. politics as we have known it. The surge of change will spell the end of the already-under-siege New Deal/Cold War elites. They will have nothing to say about *The Change,* but they will slowly begin to see how their world has failed. The technologies of the *Internet-embryo,* of the not-yet-apprehended Byte City, will make it possible for regular Americans so long disenfranchised by machine politics and plebiscitary democracy to gather and talk and act. They will gather not to nominate petty demagogues—for they will need no telegenic spokesmen—but to move, to speak, to be felt directly, as groups of citizens.

Economic revolution transforms the U.S. economy. Like the last revolution, this change increases everyone's wealth, but not everyone's happiness. The stress of social adaptation will mean a protracted period of inward-turning by the United States. As economic revolution liberates great national energies, these passions unleashed demand resolution. Like the United States after the Civil War, there will be very little energy to spare for the rest of the world—except that the revolution itself will become our connection. What we create here creates demand there. Everyone wants it; it is the spellbinding new world, the promise of a better life for billions still tied to sweatshop and factory, and billions of dollars more—like Peruvian silver bullion was to Europe's new honchos in another, revolutionary era—for elites that can bring its wonders home.[6] We export the agent of transformation: our new city high on that hill in cyberspace. The violence of our Big Change crashes and redoubles itself on them.

How "Big Change" Hits the World

There are reasons why we might expect that our economic revolution will hit others harder than it hits us. The forms of our revolution, as they are developed, tend to fit our cultural norms and belief system. America is a chaotic culture; it likes chaos, and even more important, it thrives on chaos—or apparent chaos. Beneath the spectacle others see of us, there is the same working pattern here of human culture everywhere: custom and taboo keep us all in line.

The Byte City spectacle will alternately thrill and repel other cultures. It will thrill individuals with its seemingly infinite possibilities. It will threaten their ruling classes in their guts.

The new economy the United States is building directly attacks the entrenched hierarchies of the industrial world. Late industrial rule is an oligarchic mesh of corporate-bureaucratic societies: an elegant sort of market feudalism that is both more dynamic and more meritocratic than the land-clan aristocracies it replaced. But the authority of this elite rests on the legitimacy of a system of plebiscitary democracy, which itself strictly rations people's knowledge, choices, and participation. The large corporate households—both private and public—that make up the ruling networks of our era must control information to keep the system stable. This system of control will be confounded by the absolute transparency of Byte City.

Other disruptions lie in wait. Part of the social contract that finally gave the new industrial elites legitimacy, and earned the people's trust, was their support of a social welfare system in which manufacturing workers—the majority of wage-earners—would be assured life security. And this assurance was made from on-high, by the all-caring adjudicator between people and the corporations they worked for: the ultimate corporation, the State. But in a future world in which only a tiny minority of workers actually fabricate stuff, in which corporate feudalism has been atomized, in which most people are their own economic enterprises, an ironclad equation of work with entitlement cannot be sustained. Remember, this will be an economy in which value is determined not by job status or time in job, but directly-by what one actually offers the new marketplace. People will truly make their own way, because this will be the path of biggest profit.

Thus, the elaborate industrial paradigms of Europe and Japan cannot long survive the advent of Byte City on their shores. They have weathered the first decade of Big Change-by-information by buttressing and refining their century-old social contract. Through the 1980s and early '90s, European elites did nothing to change their social welfare world. Blame part of their torpor on ignorance. They were not building Byte City in any real way—save perhaps for Japan's contribution in mortar, er, DRAM (dynamic random access memory)—so the real implications for their way of life could be brushed off as the barbaric detritus of a characteristically chaotic American life.

But part of it, at the end of the 1980s, was pure hubris. Japan, everyone agreed, was the 21st century's industrial juggernaut, and its superior products would soon sweep all U.S. markets: And did that not include computers? Europe sat back, crossing its arms in wry, historical smugness: Were they not about to unleash the world's greatest market? The European Union (EU) would soon do its own clean-up of rustbelt America—this time, it would be *le defi europeen!*

But in just the past 5 years, arrogance gave way to alarm. Japan's bubble burst, and Europe slid into unassuageable stagnation. Now, desperate yet unable to move, they await what has been happening in the United States. And they have not a clue what to do when it all rolls in.

The problem is in adjustment. The United States has already adjusted to the structural dismantling of manufacturing society. The United States has made the big investment in the new enterprises of revolution. Also, the United States carries much less of a social welfare overhead than the G-7's other six.

Consider the EU. In each European society, more than 50 percent of gross domestic product (GDP) goes to government; majority support for the welfare state is built in. Keeping social welfare means squeezing the productive sectors, but in France, marginal tax on business was just increased from 85 percent to 93 percent! Yet, even this would still work if there were enough productive enterprises to sustain the overhead. European economies need the new enterprises of the revolution, but these are so regulated that they have been strangled almost to death. EU GDP equals that of the United States, but…

- The value of its software is only about 20 percent that of U.S. software;
- The EU produces 47 percent of global manufacturing exports, but only 7 percent of the world computer market;
- None of the world's top 5 computers is European;
- None of the world's top 10 semiconductor producers is European;
- In the Euro-market, the top 4 computers are U.S. made; and
- U.S. job growth was 33 percent between 1976 and 1990; in Europe it was 8 percent, and 97 percent of this was in the public sector.[7]

Europeans buy U.S. knowledge products and knowledge services: The EU runs an $18 billion trade deficit with the United States in software. Smart Europeans who want to save on long-distance charges call a service in Oklahoma that places their *European* phone calls: They save up to 50 percent that way. They are becoming parasites of America's revolution.

Europe's elites still believe that high value-added manufacturing, like Mercedes Benz and Italian shoes, can finance the industrial welfare state. But there are no jobs in Europe and only so much value-added. The real value-added is in the United States: 50 percent of new U.S. capital investment goes to electronics and information systems; in semiconductors alone, value in terms of total capital investment shot up from 7 percent in 1990 to 23 percent today.[8] The world's cash is gushing into Silicon Valley, but in Germany, all the might of the state can't coax marks into their high-tech start-ups, which languish still as *what-ifs.*

Right now, real unemployment in Germany is well over 20 percent, the truth masked by so many unemployment percentage points stashed in perpetual job-training programs: 40 days guaranteed vacation cannot fig-leaf a job world that rations work. The head of one of Germany's largest banks, when pressed over lunch, just plain up and admitted that nothing in the end could be done about structural unemployment. Europe would just have to live with it. Then he added, as a riposte: "And what about you? Millions of new jobs, sure, but what kind of jobs? Is low-paying, hamburger-flipping such a *Brave New World* after all?"[9] A sharp point, to be sure, but work is still work. In France, where unemployment is officially 13 percent, the reality is also, like Germany, even worse: Closer to a third are jobless, if the marginally employed are counted. New French folklore fastens on the numbers of three-generation families who have never held a job.

As it barrels into this world, America's economic revolution brings social revolution. The stratified industrial economies of Europe and Japan (yes, Japan; 87 percent of Japanese workers are in globally uncompetitive companies that receive some form of government subsidy) are not prepared for the trauma that we are even now bringing to them. The old, developed world is as brittle as the thin civilization of late imperial Rome, its ruling elites as dogged as 18th-century *chevaliers facing* a rising bourgeois, and yet as helpless to stop their insatiable onrush."[10]

And what happens to the developing world? What happens to those still industrializing, still half-locked in the last revolution? If so much disruption awaits those of the G-7, those who should be ready but are not, how much worse will it be for those who still deal daily in famine and industrial pollution?

To spectral witnesses like Bob Kaplan, the future belongs to the developing world's masses of misery, where the driving force is not economic revolution, but human and environmental degradation. In his tortured landscape, cyberspace is the toy of neomedieval privilege, of a postindustrial caste secure in its pristine fortified monasteries.[11]

In fact, contra Kaplan, we can be sure that the agonies of Abidjan will not soon be relieved by America's virtual public squares—the vision of Byte City. In Victorian times too, the industrial revolution brought no succor to the slave markets of Mali. Today's transformation, like the last, begins in a single place and then fans out, staking its claim over the historical reality it has created.

Ours are like Victorian times in another way. Developing-world elites routinely, eagerly, spend their pampered youth in U.S. universities. As the architecture of a new world takes shape here, ruling elites everywhere will rush to plug in. So the net transforming American life will pull in the gangsters and warlords and languid princelings of Kaplan's forlorn anarchy.

And entrepreneurs. The economic revolution will make wealth everywhere. Like the programmers of Bangalore, the net will be a way out and up for go-getters who need not get up and actually leave. But these low entrepreneurs will be working in the United

States. They will be less inclined to pay homage to physically local rulers, and so ruling classes initially delighted will then clamp down hard.

From a Singapore Telecom exec in the know: “My government doesn’t care, it isn’t listening in to our citizens on the ‘net; but I’ll tell you one thing: Lee Kuan (and his cronies) freaked out when they were told that there were 3,000 unlicensed electronic bulletin boards on the island! That’s why we now have a national Web site. And (surprise!) everybody posts there before they post out. But we don’t listen in.” As Kishore Mahbubani, Singapore’s permanent foreign secretary, told me: “We don’t want America’s decadence, but (to control) there are other alternatives to *Pravda*.”

Mechanisms of control will be everywhere; and not all will fall. The industrial revolution that brought democracy to Britain brought new paternalism to Germany: Workers got protection, but old *Junkers* kept political power. Through the wash of peoples we call the developing world, there will be as many responses to the new as there are cultures and tribes. Those places lost today will likely stay lost. But many places full of energy—like India and East Asia—will grow in huge surges.

What is missing from analysis is how people respond to such creative destruction. Kaplan controls humanity’s outcome by reducing all our options to a narrowing circle of choices in a world aching just to survive. But economic revolution means expanding choices: more stress, but more hope too, and fertile ground not for old but for new religions.

The New Religions

Economic revolution takes time to do its disruptive work. The transformation of American life will not happen tomorrow, or next year. It was not ushered in by Windows 95, nor will it be rushed into our living rooms by set-top-box Web TV. The world we are building may only reach initial maturity—meaning an up-and-running infrastructure—20 years from now. Its impact on the world will take still longer. We can anticipate Big Change hitting Japan a bit before Europe, but both places closest to us will be upended no later than a decade after we take the first hit.

The great uncertainty rests with cultures other than our own. Even if social revolution in Europe is a calamity, it is difficult (although not impossible) to imagine the rise of a new ideology there that would in its fulfillment of new meaning demand the rejection of all things American. It is far less difficult to imagine such an outcome among cultures that historically have found fault with America. Those cultures that have suffered from contact with the West, and those that believe especially that the United States has inflicted on them a lasting degradation of identity, will be receptive to new constructions of meaning that celebrate all differences between us—and them. Even places that have been sympathetic to the American Crusade since 1945 may respond with dismay to the theater of chaos that economic revolution stages—for all the world to see—in early next-century America. Their dismay with us could have far greater historical consequences than the sum of all their current frustrations.

Kaplan’s terrible “Coming Anarchy”—like Freddy Krueger’s *Nightmares* observed in adulthood—

translates into a sordid, but not necessarily threatening, world. There are lots of unhappy people out there, but their sad slide means they have less and less with which to make us truly unhappy. Our national security problem becomes our choice to be depressed by contemplating such unhappiness.

Revolution, however, will give us a real problem. It will not only make things more interesting, it will also make them more threatening. Revolution will mean the United States has re-created economic life, but at the cost of its former world leadership and the world system it led. U.S. allies from the old paradigm will have been undercut, ironically, by their former leader, whose economic revolution has sliced their elites' authority off at the knees. Europe and Japan, plunged into an economic clearance sale, will in pain and anger begin to reorganize their societies and their politics. And those 1980s dynamos of growth, Dragons and Tigers, have exploded in their own dynamism.

What happens, simply, is the dynamic states act; they do things, try out new things, get aggressive—economically, mostly, but they remake the environment—while the old, great powers wait for new trends to gel before they follow. The dynamic states, moreover, are not the big, bovine aggregates so worshiped in industrial times—*"When China gets the assembly line, watch out!"*—but the driven communities of change. Think of Taiwan, Singapore, Korea, and pieces with an inner sense of self within China and India: Guangzhou and Bangalore. These communities are also militarily marginal, and physically vulnerable; they occupied scorned, lowly, or oppressed positions in an industrial system that exalted GDP and raw size. Their dynamism brings domestic brittleness and foreign insecurity. If we are to look for fertile ground for new religions, look no farther than the places of change.

New religions claim new allegiance. Industrial revolution created *anomie—anomie* demanded meaning. And meaning came: positivism. Marxism, socialism, communism, bolshevism, fascism.

We called these attempted new organizations of humanity ideologies. Nonsense; they were new *religions.* What is always distinctive about new religions is their passionate conviction that their truth is the only truth. A world that creates several new religions at once is a world eager for combat.

How the New Make New War

There is no point looking at the world as it is and then trying to leap to the next war. We get stuck immediately in tortured excursions that try to make of today's regime in New Delhi or Beijing an adversary we could face in combat with a straight face. For example, all ordinary trajectories hail China as tomorrow's "superpower." But this is industrial-era cliche. For example, ever since the Soviet fall, Department of Defense impulse has led it to game out 2020 scenarios of the United States and Japan locking horns with a flexing China. And why not? Their GNP will exceed that of the old Cold War allies. But we must be brave enough to say, "So what?" These are great cow states, like the Persian empire, able to raise herd-like armies that Xenophon and a handful of Greeks could overturn in an afternoon. A hundred thousand MiGs—like old Soviet iron—will mean nothing in the world of Byte City. Big empires are threatening because all those material resources await the voice of a single command. But that same single command—their control-obsessed regimes—will stifle the emergence of the very capabilities needed to wage war in the new world, the world of Byte City. So if regimes that have the will to threaten us succeed, they will not have the means to threaten. This kind of next big war scenarizing brings new meaning to the term “suspension of disbelief.”

It gets more difficult the farther out we go with the same director and cast-like a never-ending sequel to an old Defense blockbuster: *Defense Planning Guidance-DPG YXIII, The Final Agony*. There are many, many places in the symmetrical labyrinth of the Pentagon that have the word *policy* on their doors. One, “The Office of the Deputy to USD(P) for Policy Planning” shows how it gets scripted. First, the teaser: a single page that lists a bunch of interesting things that could possibly happen, way, way out: *Looking Beyond 2011*. This list, of course, contains all the things we really want to hear about, like *Cyber War and Net War*, *War in Space*, and *A Niche Peer Competitor*. But that’s the teaser. “The consensus is…” it says, as though the subtext should read, “that these things are so far out we don’t have to talk about it; we just wanted you to know it has occurred to us.”

The plot lines we actually get to look at are somehow familiar: *“Sarajevo 2011,” “Just Cause 2011,” “Strait of Hormuz 2011,” “Counter-Terrorism 2011.”* See what I mean? There are more surprises on *Nick at Nite.* Planning tells us to take today’s snapshot—with all current trends holding—to some arbitrary, even-numbered date called “the planning horizon.” This gives us Beijing or New Delhi with *x+y* number of weapons more than they have today but us with the same, disbelieving face.

There will be no new war without new religions—just as there can be no revolution without a disruption of meaning. That disruption has already begun, and so new religions are ensured. It is today's stale, crust-brittle constructions of meaning that are not long to crumble.

You don't believe this? Why are we so shocked by Serbian blood-vengeance, Chechen blood-vengeance, Algerian blood-vengeance, anybody's blood-vengeance, but not by our own lack of awareness of it?

Our elites take pride in denouncing these passions as primitive, dismissing them as deviant: If they can't be put down, they should be condemned. These same elites have no sense of the authentic source of these passions—a demand for meaning in a world in which stability and order have been ruthlessly stripped away—and these passions' abiding power—to fight starving in the snow at 30 degrees below zero, to make yourself a living bomb, to head-shot prisoners one after the other, without flinching, because they are The Stranger. We watch, heads shaking, as the edges of civilization slough and scale, and we feel nothing but scorn and superiority.

The shock will come when it all hits home. Does the lamentation among the elite over the sordid death of Tupac Shakur, and the high-gloss sackcloth-and-ashes covers like *Rolling Stone* gave him, give us a little clue? None of us can analyze what coming apart means in our own society—we are all too close to it ourselves. But we feel it, even if we don't talk about it. And we know too that Bill Bennett's *Leading Cultural Indicators* are no more than modern, shamanistic prayers, in a time when the old shamans have all gone.

It is not to be discovered in our society's dismal data: How many in the penal system? How many illegitimate births? How many single-parent households? Things fall apart when the old belief system no longer wants to defend its values and its ways. New religions succeed because they do believe. How they believe!

The shock at the violence of new religions—unlike our contempt for today's brutal tribal chant—must be the shock of recognition in revolution itself. Part of the experience of revolution is overcoming that shock. Eventually, we will accommodate to upheavals at the center, and they will seem different to us because they happen here, or in places that we have long ago decided are centers of civilizations: Not Serbia, not Daghestan, but Japan, France, China, the United States.

Revolution takes war away from the margins, from tribal splatterings at the limits of what we control, and puts it back in the firmament of the center, among close relations, in the heart of the world metropole. Revolution so changes the world *bourse* that nothing else can stay the same.

Americans will accept conflicting new religions in a world after economic revolution runs its course. We will surely have run a course with many homegrown cults and religions of our own. But we may be less ready to deal with triumphant, inimical movements that have us directly in their sights.

By less ready, I mean less prepared to deal with the fruits of their animus against us. Today, we chafe at the prospect of highly motivated, Islamic revivalist groups doing their worst on us, but compared to the potential power of a great new religious movement, drawing strength from its millions and the surging technologies of revolution, these zealot clusters are nothing. If new religious movements, like the Nazis or Bolsheviks of this century, claim the energies of whole peoples—passionate, educated millions—then the new world and its new meaning are really worth worrying about…

War Celebrates New Meaning

…Because Nazis and Bolsheviks practiced revolutionary war. We thought they meant revolutionary, as in radical, red ideology—a grim perversion of modernism—and it was that, on the surface. But it was revolutionary in another, more disturbing way. Their wars, especially Adolf Hitler's war, were a religious rite of passage. We never allowed ourselves this insight, because it would have been too frightening to bear; it was scary enough, after all, to think of Hitler and Joseph Stalin like Genghis Khan or some other savage, and preferably oriental, conqueror. But a new religion, springing out of Western tradition, out of modern thought, in the land of Luther and Hegel? And not just the cult of some newsreel Svengali, but a new faith taking root? Too primitive, too existentially threatening, to address consciously at the time. But we did find a way to get the message in our gut, by recognizing the power of their totemic symbolism.

We still think of Nazi Germany as somehow keener on new technology than we: better tanks, guided missiles, jet planes; forgetting that we pushed the technology envelope far more in our "Good War" than they. "German scientists" became Cold War slang because of what science and technology meant to the then-new *-isms.* Then we shivered over *Sputnik* because of the meaning Soviets invested in war's technology. Soviet and Nazi religionists used the sharpest badges of modernism—high-tech weapons of war—to celebrate (and make us believe in) the inevitability of their triumph: hence the new-wave Panzers and hot Heinkel formations of a Leni Riefenstahl newsreel or intercontinental ballistic missiles grimly rumbling across Red Square became the totems of new meaning—publicly, flamboyantly celebrated. Hitler's and Stalin's cults were receptive to new war because new war could be used to insinuate emotionally the conviction that their vision, their belief systems, were about to be unconditionally fulfilled.

We have come to see war in stark contrast. We permit ourselves some modest, tame association of war's technologies with our own belief that mastery of such technology shows a kind of natural superiority, but then we go and drown this almost-celebration with apologies in advance of its demonstration. We have done this too in historical retrospect, stripping former celebrations even from the Good War, even on its fiftieth anniversary. To us, war can never again be a celebration. It is at best a profession.

Why does distinction between wars matter? It matters because war for us serves a very different purpose than war for them. This is the heart of the difference between status quo war and revolutionary war; and it is the heart of the difference that matters much more than the visible things that seem to make war.

Revolutionary war is not defined by revolutionary weapons, just as status quo war is not defined by status quo weapons. The weapons of war, and the way war is made, are vehicles for realizing what this war represents, and in fact, what it is: *Revolutionary war is the celebration, the realization, of identity*.

This was true for the Hitler cult especially. It is important also for us to understand how we defeated revolutionary war then. The United States met revolutionary war—the celebratory war of the new cult—head-on, with a messianic fervor of our own. We made of world war a *crusade* (in Dwight Eisenhower's words) and used the power of American movies and American music to infuse our "war effort" with a religiosity of passionate commitment and fulfillment. The power of mass, religious mobilization can be glimpsed in the thrill Americans felt when hearing of Hiroshima. The Good War built up enough messianism to carry us through a dreary and depressing Cold War, 20 years and more down the road, all the way to Vietnam.

Revolutionary war as enacted by the Hitler cult is worth remembering because it was done to us. The thing that is to be feared in our future—from the new religions—will not resemble the Hitler cult; but war will have the same, celebratory purpose. For the new religions, war will be essential to their becoming. The very experience of war is realization of the new: You create yourself by destroying the stranger.

This is why it is important to recognize the religious dimension of Nazi, Soviet, and American war. If the Good War gave the United States its Cold War momentum, the Great Patriotic War did even more for the Soviet regime. It became the treasured, sacred experience of the Soviet state and its peoples. It may have been the only shared element of meaning holding up the rotten Church of V.I. Lenin in its last decades.

We, like the old Soviets, finally lost the talisman of the Good War. Vietnam destroyed it, and young generations have all but forgotten it. A half-century of Cold War slowly turned its back on the very celebratory Good War that immediately preceded it. Part of this was blamed on the atomic bomb, but there was more at work than that. Things military became tied to a social order: its own caste studiously, and with excruciatingly care, niched itself into the larger hierarchy of those who ran the Cold War, and Cold War American life. Now there is no longer an American Way of War in a national, and certainly not in a religious, sense. War has become a toolbox owned by the ruling establishment. For the American overclass, war today is a reverse affirmation of everything that can be lost. This is classic status quo thinking, of course. War is something *not* to be fought, but its tools are always to be *used* in support of that same status quo.

But preserving the late 20th century American status quo is far different from France or Britain preserving the mid-19th century status quo. The difference is that Americans do not like imperial wars. Therefore, the Washington ruling establishment must manage by demonstration and awe. This means maintaining very high force levels for world management purposes, even in the absence of a major competitor. These forces must be constantly and bullishly in play—in operations other than war—and yet still not used. This helps to explain why any successful war activity is immediately and loudly trumpeted as an advertisement for the national security subculture (which includes defense industry and other civilian constituencies) as a whole. In the face of domestic uninterest, a world management force must be sold to us on the basis of a carefully crafted package that combines residual nostalgia for the Good War crusade and a coded message about preserving U.S. military superiority. The message of this management-oriented policy is that *We must stay on top—in control—or we will lose.*

The unintended emphasis, strangely for the superpower, is on losing. To get the current force levels it wants for management, the ruling elite must insinuate the notion that any retreat from these levels is a historic loss or retreat for the American nation. To send this message—as untrue as it is—these same elites must strike a tone of pessimism, even defeatism. This mental stance is the starkest contrast to the unbounded optimism of the religionist bound for revolutionary war: *The future belongs to me*.

Sea Beggars and Lions of the North?

You want to know what they will look like, the enemies that come after Byte City? You want to know who will fight in the great ether—fired by revolution's passions—better than we? I have chosen metaphors—stories—to talk about war and Big Change, because analysis (the reasoning language of our era) can tell us only about what we know; and the change is beyond what we know. How industrial revolution brought surprise, and defeat, to France, is a metaphor for us. Industrial change brought wars of bigness, and from the Civil War to Desert Storm, the United States has been the master of the big war. But if we want to go looking for a good metaphor for our next enemy, we should not look there.

The next wars, the wars of bits and bytes, may not be about bigness at all. And we can find a metaphor for how the small overcame the big in the revolution of the 16th century. We could call that the Mechanical Revolution, because it gave us gadgets like the printing press and the power loom. It also gave us the tools to find and conquer a new world: ships and cannon. And it was these "engines" that changed war. Two places excelled at making them: Holland, for ships; and Sweden, for cannon. Both places were small: each was about one-twentieth the size of France, Europe's longstanding superpower. Both lived at their world's margins: Sweden was a minor power, and Holland did not officially exist at all.

Yet for a time, quite out of nowhere, Holland and Sweden became Europe's dominant military powers. Part of their power was that they were primary producers of the new weapons, and for the Dutch especially, civilian manufacturing could be converted directly to war. But much of their power came indirectly, from the thinking and the habits that led them to make so many ships and guns. The new manufacturing's management skills gave them an edge in operational art: It helped them to make war better. It was not coincidence that the two greatest war minds of the early 17th century were Swedish and Dutch: Gustavus Adolphus and Maurice of Nassau.

But there was also what could be called a cultural nimbus-effect—the energy of mind that gave Holland and Sweden the power tools and the know-how to use them also drove them passionately to put them to use. It was the 16th century's Big Change in meaning—the Reformation—that fired up Holland and Sweden, and that made two tiny societies for a time indefatigable on the battlefield. Ideational change animated the material changes of the Mechanical Revolution, and the new meaning unleashed was like a halo, an atmosphere infusing successful action.

“Sea Beggars” and “Lion of the North” are our last fragments of common historical memory from those times. But they are remembered because they recall the absolute mayhem and rebellion that Holland and Sweden visited on Europe: the swagger and genius in war that brought the Habsburg superpower to its knees, and that made of Protestant heresy the European future.

To move all this into our own future, *look for the rebel city states of Byte City.* You ask, *“Could they be contiguous communities, like those high-tech city states on the East Asian rim?”* But suddenly we are back to old think, and within minutes, someone else will start wondering whether Singapore could ever pose an “information-war threat.”

This kind of thinking misses what actually happens in revolution. Go back to the 16th century for just a minute. The high princes of that world—like Prince Philip, visiting the Netherlands in 1549—would see the Bishophric of Liege, or the Lordship of Friesland, or the Duchy of Gelderland.[12] This was where he was. That was what it was. Like Phillip then, we see only a world of industrial-era nationalism. Everything is defined by the standard of the nation-state, so things that aren’t officially states are called “nongovernmental organizations,” or factions, or militias, or sects.

If the next enemy is not a big place of industrial iron—like China—it is not necessarily a dynamic small place—like Singapore (which our Defense guys, I suppose, would call a “niche peer competitor”). The next enemy as a *place* does not yet exist. It first must be born, and its birth will be its consciousness of self. Holland became a threat to Habsburg Spain when it became Holland. Its superior tools and mind were not the threat, they merely allowed it to win.

Perhaps part of the problem *is* that the new place itself does not yet exist. That place is perhaps 20 years away; but with the coming of Byte City, it will be easy to see how people and new meaning will gather there. And above all, though it will call itself a marketplace at first, Byte City will be the place where new societies can realize themselves. Because Byte City, as the grand world bourse, will encourage trading in ideas and meaning as much as in services and commodities.

The problem for us is that, as the hegemon of the status quo, we will be the one discouraging new nations; our energy will increasingly turn to regulating dangerous ideas; and our power will go to controlling heresies that threaten the “stability” of our world system. So we should find our next enemy in those communities of passionate ideas struggling for political liberty, or in messianic movements that reject our system’s dominating legitimacy. And unlike those who feel that rage now—the detritus of older cultures’ religions worn down in colonial wars with industrial Europe—those who will challenge our authority successfully will come from the new religions that percolate with Byte City itself. Their challenge will be coexistent too—both in the digital and material worlds—because the digital will by then be interwoven into our lives, the weave itself weakening old-style authority.

And though we may call them “Sea Beggars”—or “Terrorists”—they will not be anything like those semi-medieval Islamists we know, fumbling with the killing tools of the modern. New tribes will effectively challenge us because they will be the ones that create the tools of a new world, the world after the modern —the next Holland, after the next Luther, after the next Gutenberg, building Byte City.

Why We Stay Stuck in “Old Think”

It’s not surprising that we stay stuck, because the Old Establishment will resist Big Change everywhere.

Defenders of the world status quo, the Cold War elite is visibly hunkered down in its final *Plaine du Jarres* command post.[13] America’s current national establishment was crowned in crisis. Exigency equaled authority, so Cold War became the perpetual crisis that demanded a perpetual imperial ruling class. And it is a big, messy world out there. Even when the big crisis—the Cold War—died, there seemed so many out there to take its place. Change was always out there and always bad, which meant always good—for the elite.

But the onset of Big Change within the United States is like “The World Turned Upside Down,” the denouement-tune Cornwallis had played at Yorktown.[14] Elites have no authority to defend against, let alone define, domestic change as a threat to national security. It is simply a threat to their own security: the security of their position.

This happened to another elite; actually, it was Cornwallis’ social set that got hit, a couple of generations after Yorktown. Like America’s overclass, they came out of 40 years of war (with a short break in the 1780s) only to find the real threat to their authority was from their own people. Methodist preachers, mill owners, Spenlow & Jorkins, Marley and Scrooge —a new elite was rising and taking over their world.[15]

So Washington’s *ancien regime* channels its response to world change, and to a world revolution that is American-made, into rigid, familiar paths, with the unconscious complicity of America’s military societies. Hence the desire to level Byte City–-that wide-open town—turning it into an Information Superhighway, the ultimate toll-and-control road. Hence the urge to embellish “terrorism” to the point at which national security becomes a domestic problem. Protecting societies created for Cold War by finding new (and often, internal) threats, new structures of “security” to impose at home, carries with it faint whiffs of paranoia. But it pays the rent.

And the leading corps of our military societies see some of this, as a dense and dangerous thicket for their people, but one they must enter nonetheless. And they seek, with all the nature and honor embedded in their ethos, to bring everyone out on the other side. Their watch has marked the beginning of that dense and dangerous peacetime. They have chosen to cut for themselves three characteristic paths through the thicket or footpaths to the future, called Readiness, Reform, and (R)evolution.

Readiness

Readiness is an identity-mindset; it is not simply semper paratus. The readiness ethos includes a strong dose of “we must be ready to go,” but its sense of itself more closely corresponds to Hamlet’s “the readiness is all…” Its world is a world of imminent combat, in which the only things worth doing are those that might happen tomorrow or maybe even tonight. Readiness’s wars have already been fully apprehended, because they have already been fought.

Readiness is a worldview that believes in the robustness of control. Things can be managed, and change can be held down, as long as we have the means. Readiness is the predominant peacetime ethos of the defense world, because it appeals to what most everyone wants; to keep doing everything they’ve been doing, forever.

One good opinion gives us the flavor of a true on-top, status quo mindset:

> *The lessons and revelations…of the Persian Gulf War victories…mandate that a new style of warfare will be employed in future elective wars. Technology offers the leverage that facilitates the accomplishment of the new expectation imposed by the American public. Our military can win decisively anywhere in the world. It can defeat an adversary anywhere in the world* (sic) *in reasonable amounts of time. The day of long drawn out warfare has past* (sic)*. It can take battle to an enemy and with the proper technology minimizes* (sic) *our own casualties. It can destroy an enemy on the battlefield while preserving, should it choose, the country, national treasures and way of life of that enemy.*[16]

This quote was chosen because it represents, errors and all (it is, after all, an unabashed draft!), an authentic attitude rather than a massaged, politically disinfected, nearly meaningless official statement. The world of our military's predominant Readiness ethos is the majestic world of absolute mastery. This mastery must be maintained so the threat to it cannot be the minor criminals and thugs that it uses to justify its splendid state. No, the threat is any bigger change in the environment that threatens the most comfortable nest any military society has *ever* inhabited. (We think of ancient Rome as living for centuries in a state of free security. But name one *decade* when Rome's legions could afford to relax—when they were not at full stretch!).

So Readiness defines the current enemy as the always-enemy, because within its reasoning, no big enemy could arise as long as the superpower manages world conflict. "Deterrence" migrates in this mindset from a relationship designed to maintain a permanent nuclear status quo, to a relationship in which vicious but smaller regimes and bigger but more benign regimes are both "deterred" from challenging a permanent American world status quo.

The quote's emphasis on the Gulf war as model is also a feature of the predominant path. It implicitly freezes war by codifying modern war as the last victorious engagement. This has the benefit of freezing as well the institutions, relationships, and force structure that fought that engagement. Modernity is carefully contained within the realm of things that do not threaten institution, relationship, or force structure. So new technology—and by extension, research and development (R&D)—is channeled into the development of high-tech badges, refinements, or appliques to existing weapons phyla.

Reform

Reform's urge follows cherished American tradition. U.S. military reform—groping after and mirroring contemporary reform movements in American society—seeks to improve bureaucratic performance by improving efficiency. This is pure *perestroika*. It is everywhere now among imperial bureaucracies frightened of mandated downsizing. "Reinventing Government" is perhaps the best tag line, because it captures the spirit of Reform: make it work a little better, make it look a little smaller, call it something different, but above all, keep it the same!

Intrinsic to this process is the demonizing of corruption and inefficiency. The core belief is that efficiency is the desideratum: the thing most wanted. Efficiency solves peacetime problems. It allows us to fight future battles without increasing today's budgets. It is progressive in the sense that it brings military society in sync with what is considered better and more modern in the current American spirit of the age. Admiral William Owens thus belongs to the lineage of all American reform and symbolizes military society's harmony with all of American society, just as Elihu Root or Admiral William Sims brought their services in tune with the progressive spirit of their day.[17]

But this path is more of a response to domestic change than it is preparation for future war, and it creates its own cultural backlash. The example this time is from a reform briefing by a former Defense Department official in 1995. The chart is entitled "Achieving a

Common Futures-Oriented Framework For Defense Decision-Makers." The chart correctly—even powerfully—identifies one of the deepest elements of corruption in the Department of Defense: the swarm of interest groups whose competing needs must be resolved before any policy or budget can be made. The chart shows the thick alphabet soup that must be adjudicated before even thinking about the future can happen. And the official was fired for trying to do something about it.

Reform, far from simplifying and sorting out the mess, often only adds to it. The Joint Staff should have replaced several layers in the bureaucratic pastry, like the service secretariats. Instead, it is now yet another layer. Unless reform is the central agenda of the highest authority, executed ruthlessly from above and responding to a widespread sense of crisis, indeed, a public outcry for change, it only succeeds in creating yet another internal interest group to be fed. Witness Prussia's military reforms after the calamity of Jena-Auerstadt; or, lest we forget, France's after Sedan. So reform's fulfillment waits, often until peacetime's end, for crisis to make it happen.

(R)evolution

Military "revolutionaries" within a peacetime status quo elite tend to focus on new weapons. It was true for the 19th century French; it is true for the "revolution in military affairs" guys today. They love to imagine a totally new weapon that replaces today's dominant weapon. Surely, that's a revolution. Carrier replaces battleship, tanks replace trenches. But their thinking reveals not revolution, but passionate conservatism. Why?

For one thing, they can not even think about bucking the dominant paradigm: preserving the status quo. They would quickly be punished or banished to the most terrible hell imaginable for thinkers—obscurity—if they even suggested that military change means deconstructing the old paradigm itself. But then, even in obscurity, they could at least call themselves (R)evolutionaries. So focusing on weapons is politically safe. And if technology change, which surely accompanies revolution, is big enough, then it actually becomes the entirety of the change itself. And the new weapons it brings *come to be seen as the revolution itself, when in fact they are only a substitute for it — and thus no threat to the society the weapons uphold.*

A public example of this phenomenon (from someone who was once part of the Pentagon's only officially sanctioned cell for (r)evolutionary thought) is Andy Krepinevich's "Funding Innovation: Low-Cost Operations for Leveraging the Military Revolution":

> *…in the 1920s, the U.S. military successfully laid the foundation for success in the next great power competition by "reinventing" itself in response to the geopolitical and military-technical revolutions then under way. During the 1920s and 1930s, the military services positioned themselves to engage in new and different kinds of military operations—strategic aerial bombardment, amphibious assault against stoutly defended positions, and carrier-based air strikes. And they did it on shoestring budgets. Denied the opportunity to think "richer" about defense, the military services thought "smarter."*[18]

Krepinevich is right about one thing: The U.S. military did think smarter—about what was already in play. There was no revolution during the 1920s and ’30s. What was introduced in the Great War just got worked on. Airborne assault, armored maneuver, carrier task forces, aerial bombardment, wolf packs—the whole repertoire of the second war was rehearsed in the world’s collective military mind after the first, year after year, for 20 years. It was just that some thought more efficiently than others. But as real war, the second differed from the first merely in embellishment and in efficiency. It was better theater, but there had been no revolution.

Yet how advantageous to say that cruise missiles or stealth technology or microprocessors have “revolutionized” war! Self-styled (r)evolutionaries can appear to take on the Colonel Blimps of the readiness mindset, saying they are cutting R&D and merely building the forces of yesterday, while in reality never threatening either their position or their mindset.[19]

Perhaps the trendiest fashion in revolution is blending “chaos and complexity theory” into official doctrine. New thinking in the natural sciences is daily changing how we understand our reality. But, as Alan Beyerchein points out, Prussian general Carl von Clausewitz was suggesting some of these same notions at the beginning of the last world revolution.[20] Larding ops-speak with “attractors,” “complex systems,” “the ecology of the battlefield,” is no more than a hip remix of an old song, *if the lyrics themselves don’t change.*

The old song is our concept of the battlefield itself, and of preparing for battle. The (r)evolutionary still approaches the battlefield in peacetime as Clausewitz must have, as a pedagogical abstraction, protected from the outside world—as something which, through prodigious study, could at last be mastered. In their minds, the battlefield is to be changed by them—the owners of war—through sheer intellectual effort. But war is being remade today in every place outside of war; and it is every place having nothing to do with war that will shatter, and then remold, the battlefield. It is not chaos and complexity on the battlefield that the revolutionary needs to study, it is the chaos and complexity of Revolutionary life.

(R)evolutionaries are in this way much like reformers: they want to make the current system better. To the reformer, corruption translates into the sloth and obesity of the system. To the revolutionary, corruption translates into "old think" about fighting war. But the system, meaning the prevailing paradigm that encompasses the physical, the institutional, and the ideational aspects of a war society: The system escapes all rethinking.

And what is the system? It is the cultural sum of war: the military societies, their institutions, and a whole way of life. But it is more even than this. It is a belief system, an existential way of thinking about one's own identity and the reality that it inhabits. So any current example of (r)evolution because of its own existential limitation of mind, cannot even come close.

A jewel-like example is posted on the World Wide Web for all of us to read. It is entitled, "Leveraging the Infosphere," and it is the U.S. Air Force's vision of military revolution. The digital paper begins by showing its high-tech credentials, as it ticks down a gee-whiz check-list of all the latest gadgets, from DNA tracking to hyperspectral sensing to taste scans of targets from space.

The paper ends with its own taste of the future, in which we glimpse a theater commander in chief (CINC) as she conducts military operations in the Air Force's infosphere. She sees everything from her remote command post, every grunt in every platoon, and, we are told, "they could even have loaded DNA data on the opposing commander into the Data Fusion Control Bank (DFCB). The Infosphere itself is a mighty, pristine, and untouchable deathstar called the Global Surveillance, Reconnaissance, and Targeting (GSRT) system. Who could ever challenge such military majesty? "As each warrior [sic!] requested target data, GSRT fused sensor data, tapped data bases, activated resources, and passed templated neurally collated information to each person in exactly the format they needed to get a clear picture of their enemy." Of course. The perfect scene ends, as the "CINC paused for several moments, wondering how battles were ever fought without the information systems she now used with practiced ease, and she was glad they were fighting an enemy still mired in the visual/ELINT [electronic intelligence]-oriented maneuver force of the last war."[21]

This is not revolution, this is *Star Trek: The Air Force Generation.* It is futuristic from the retro-vantage of the industrial age: like the sci-fi oxymoron, "space dreadnoughts." It is a war world still ruled by its physical devices—now active in the electronic ether, but spiritually still mired in a mechanical world, where our devices fight their devices. More important, even: It is a world in which military societies still fight much as they do now, but with the added data-realization the Infosphere gives us. The

Infosphere thus ends up as just another medium—another dimension—of the battlefield. The idea that the world infosphere becomes the next human place; that to fight there we might actually have *to be* there, where people are; and that the enemies we face in the digitized ether may have the edge on us, do it better there than us—is unimaginable.

None of this presumes that those defending any of these three paths to the future are moral invertebrates, corrupt of mind, or alien to honor. They are serious people, the finest we have, whose thinking is leashed by a system that permits them to address only part of a problem, to analyze these pieces in strict mental compartments, and to assemble them at their peril. The system that controls thought is neither conscious nor deliberate; but it is enfolding. Remember, it is a complete belief system. So when the rhetorician asks, "But where is (R)evolution?" We must answer that it simply cannot exist—at any level—until the larger revolution spends itself sweeping our old way of life away.

Here the French analogy, full circle, holds little historical comfort. The French, like us, had their military trajectories in mind. They had their predominant path to the future, and it, too, was readiness. If we took back to that world of 1860, the French had a splendid army that could do everything the empire asked of it. They were ready to fight the Russians or the Austrians all over again. They had their *jeunes ecoles,* product of *grandes ecoles,* fighting for reform, efficiency, purity of command and operation. And they had (r)evolutionaries, engineers whose visionary weapons promised to hold the key to future battle. And none of the paths was wrong. An ethos of readiness made the French army the most combat-honed force on earth; an ethos of reform pushed France at last to respond to the Prussian threat; and an ethos of (r)evolution gave the *armee de la grande nation* the "techiest" tools of war.

As separate mental footpaths to the future, however, these paths would meet, finally, only on the field of defeat. Reform bested readiness too late, and the big army reforms that followed the shock of Konniggratz, and Austria's stunning defeat in 1866, only served to throw the French army into confusion. France went into battle in 1870 not knowing itself. Reforms pushed in a hurry only robbed old veterans and commanders of the confidence they needed; they did not have time to find something new to believe in. That necessary something new was a new vision itself, not just the intellectual appliques of new battle manuals and new tables of organization. And how could *l'armee* possibly create a new vision of itself in time, when it had not taken the time to know war: how war was really changing; how the new world was machining it, reengineering it, so that it became something new.

We have several steps to take before we can begin to know this. The first is seeing the real change, and accepting the irony that we are making the revolution that will transform the world. The second step is connecting a transformation in life to a metamorphosis of culture itself, and then of war, which is culture's creature. The third step is confessing that, although we begin the revolution in life, others—their red dreams not yet imagined—will begin the revolution in war, because war will be both their celebration of birth and its realization.

If these recognitions were all we needed to begin the road to the next war, we would already be into the journey. But there are other obstacles, the antirecognitions of denial, that are more intractable, that hold us in place like little trees with long roots.

- Our hallowed record of historical success: *Why question it?*
- The long time since we met a real competitor: *Who is this upstart?*
- The comforting feel of ongoing "reform:" *Been there. Did that.*
- The power of our national myth: *We will always rise to crisis.*
- The talisman of triumphant technology: *But we have the Death Star!*

So we await our Sedan. To dismiss this prospect, we must dismiss the possibility of a future foe, an equal challenger with evil intent. To dismiss this possibility, we must dismiss the transformative power of Big Change and assert that we can keep control not only of our world system, but what happens to it, forever. But no one can do this.

So we await our Sedan.
This much is certain:
The only uncertainty
Is in its outcome.

[1] Why verse? I liked the way it looked; I felt it would pull the reader in with image as well as argument. But then others who read it said: This is not serious! Not in a policy journal! So a simple impulse took on more difficult overtones. I thought, maybe such resistance to mere reformating is a sign. Because in revolutionary

times, the old rails not just against new existential thought, but against new talk, too. Before the industrial revolution, people often wrote in verse. But after Newton and the emergence of the industrial-speak we call analysis, poetry died as part of daily discourse, so deconstructed at last as to drop like Latin from our language. But part of what is happening now, urged on by new metaphors in the natural sciences, is a search for ways of expressing thought that analysis cannot reach. Think of this verse-fragment, snatched so easily from prose, as an historical reminder: That how we talk will make revolution as much as its gadget-flash.

[2] Prussian General, later Field Marshal, Helmut von Moltke, modern war's creator, is still remembered in the popular cliche "war by timetable."

[3] I am indebted to Dennis Showalter for his insights into mid-19th century France and its army. Perhaps his best-known work is *Railroads and Rifles: Soldiers, Technology, and the Unification of Germany* (Westport, Conn.: Archon, 1975). He also graciously allowed me to draw on an unpublished manuscript on the French army before 1870.

[4] This doubling-CPU (central processing unit) slope is a line ubiquitous now to every briefing on change. Carl Builder's November 1995 RAND briefing, "Peering into the Future (Looking for Shapes in the Fog)," brings a sense of our own expectations in one chart, "A Century of Computing," which indicates a sixfold increase in orders of magnitude, if the 50-year trendline is extended to 2030.

[5] The argument for this idea is made most forcefully in a lyrical passage from Peter Huber's reverie, *Orwell's Revenge: The 1984 Palimpsest* (New York: The Free Press, 1994), pp. 171-181.

[6] Spanish silver from great mines like Potosi fueled Europe's mechanical revolution of the 16th century. Fernand Braudel illustrates how Spain's New World treasure "escaped from its coffers and traveled all over the world," mostly to the new place of revolution: the Netherlands. See Braudel, *The Mediterranean and the Mediterranean World in the Age of Philip II* (New York: Harper & Row, 1972), pp. 462-542. Like Spain, our networks and our software will flow to opportunistic elites everywhere; this time, instead of bullion, the fuel is bits and bytes.

[7] From Gary Geipel and Robert Dujarric, *Europe 2005: Turbulence Ahead, an Executive Briefing* (Washington, D.C.: Hudson Institute, 1995), pp. 8-9.

[8] See the tables in *Economist*, August 27, 1994, p. 60; and *Wall Street Journal*, November 14, 1994, p. R18.

[9] Anecdotes on Germany and France come from discussions with Dr. Deltlef Marquardt, DG Bank, and Pascal de Jenlis, one of France's preeminent entrepreneurs.

[10] When Louis XVI convened the Estates General in 1789—the event that led to revolution—Jean-Paul Rabaut Saint-Etienne, a Calvinist politician and pastor later guillotined, described the scene, and the sartorial effrontery of the high estates in the face of the people:

> *The senior clergy, glittering with gold, and all the great men of the kingdom, crowding around the dias, displayed the utmost magnificence, while the representatives of the Third Estate looked as if they were dressed in mourning. Yet their long line represented the nation, and the people were so conscious of this that they overwhelmed them with applause. They shouted "Long live the Third Estate" just as they have since shouted "Long live the nation!" The unwise distinction had produced the opposite effect to that intended by the court.* (Quoted in Jean Starobinski, *1789: The Emblems of Reason* (Charlottesville, Va.: University Press of Virginia, 1982) pp. 17-18.)

Today's elite etching is less class—and cloth—conscious, but can we imagine a similar scene in digital tailoring—of old and new elites clashing in tomorrow's Byte City?

[11] Robert Kaplan made a searing impact on the late-industrial imagination with his 1994 article, "The Coming Anarchy" (*Atlantic Monthly*, February 1994). As I suggest, Bob Kaplan is really a latter-day Victorian adventurer, a romantic. But his portrait of what awaits us appeals to the ancien regime because it ratifies the need for their continuing authority. By implying that there are only two possible world futures, elites get out of Kaplan a stark, but highly comforting, "either-or" message: "Either we in the West manage the world, and ourselves, more effectively, or the world subsides into barbarism; like that time after the fall of Rome, the long twilight of civilization." The old world order does not want to hear about dynamic new worlds arising from culture's chaos, or of the West reinventing itself in cyberspace. It wants the siren call of the White Man's Burden, suitably updated, purged of bad language and made squeaky clean politically correct for our post-modern sensibilities.

[12] This Philip was, of course, Philip II, the demon-to-be of the Netherlands' Seven Provinces. His visit and its ironies are nicely summed up in Geoffrey Parker, *The Dutch Revolt* (Ithaca, NY: Cornell University Press, 1977), pp. 19-30.

[13] Dien Bien Phu, a very small place on the Laotian Plaine du Jarres, was the site of yet another French debacle. Americans remember the fall of Dien Bien Phu because it started us on the long road to Vietnam, which became in the end the central passion of the Cold War itself. From the newsreels of 1954, Americans watched the beleaguered French defenders, surrounded by "hordes" of Viet Minh, holding on to nothing more, at last, than a single, lonely command post.

[14] General, later Lord, Charles Cornwallis, like Britain, recovered from the loss of one great imperial jewel by rooting about for another. Cornwallis would become, after Yorktown, Governor-General of British India.

[15] Two sets of characters from Charles Dickens—Spenlow & Jorkins from *David Copperfield*, and Ebeneezer Scrooge from *A Christmas Carol*—etch our memory of the new men who overturned the economy of squire and trader (like poor Fezziwick!).

[16] From an unclassified draft chapter presented at a highly classified 1993 Department of Defense conference. Its title: *Directed Battle, A Vision of the Future*.

[17] The first line in Admiral William Owens's book, *High Seas: The Naval Passage to an Uncharted World* (Annapolis, MD: Naval Institute Press, 1995), reads: "This book is about change and innovation in military institutions." So he deliberately announces himself as the Reformer. And like his Progressive Era progenitors, he shows an urge to achieve what might be called controlled modernity. At the beginning of this century, Admiral William Sims sought to make the Navy shoot straighter, only to find that a more efficient fleet first required modern thinking in its ruling bureaucracy. To do that, he needed to link up with the reform zeitgeist sweeping U.S. politics—he went straight to the President, to Teddy himself. Like Sims, Bill Owens sought to remake the Navy by changing its bureaucratic ethos—"living jointly"—and exploited political support from reformers on Capitol Hill and in the White House. The sense of "controlled modernity" they both sought is to be found in the orderly and symmetrical visions of efficient, modern navies their reforms would sire. The change they wished to respond to, and champion, was itself thus carefully orchestrated: *their* innovations, *their* change.

[18] Andrew Krepinevich, *Funding Innovation: Low-Cost Operations for Leveraging the Military Revolution* (Washington, D.C.: Defense Budget Project, 1995).

[19] Perhaps because the Colonel never existed, his name can be called on, and substitute perpetually for those we really want to finger. No one ever calls a four-star general or Commander in Chief a Colonel Blimp; instead, polite (R)evolutionaries at Court talk through historical metaphors, as though they were characters in a Japanese Noh play, sending their messages through stories about the obstacles Admiral Jackie Fisher faced trying to bring revolution to the Royal Navy a century ago.

[20] Alan Beyerchein, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* (Winter 1992-93), pp. 59-90.

[21] "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020" can be found at http://www.au.af.mil/Spacecast/app-b/app-b.html

CHAPTER 4

CAN INFORMATION WARFARE BE DETERRED?

By
Stephen Blank

Can information warfare (IW) be deterred, and, if so, how? To pose these questions suggests that we can extrapolate from prior understanding of either conventional or nuclear deterrence the means to deter IW and future attacks using information technology (IT). However, we must also admit that this question suggests that this assumption may be unwarranted. It may not be possible to deter IW with existing concepts and mechanisms of deterrence. Moreover, this way of posing those questions suggests that the United States is no alone in searching for answers to them. Other states including potential adversaries are also doing so.

Thoughts on Deterrence

Although U.S. writing on deterrence could fill a library and has profoundly affected international strategic thinking, this does not mean that all answers to these questions must follow U.S. models of deterrence and IW. To assume that other governments must follow in the American wake is the height of ethnocentrism. But sadly, much of the writing in the U.S. about future war, IW, and IT exudes ethnocentric triumphalism and disregard for other countries' military traditions, thoughts, and practices.[1]

Nor is it clear which previous model of deterrence pertains most to the problems raised by the advent of IT and IW as decisive strategic factors in war and peace. Deterrence models are almost as numerous as the authors who write on deterrence and there are now attempts to extend that concept even to low-level conflicts like Somalia.[2] Such model-building far transcends the original efforts to derive a theory of deterrence for nuclear scenarios. In the United States, opinions abound as to whether a nuclear or a conventional deterrence model is the appropriate analogy for IW or for future war in general. Three opinions have emerged from the debate around this question. Admiral William Owens and Dr. Joseph Nye, two former high military-political officials of the Clinton Administration, argue that just as nuclear superiority conferred military dominance upon the United States after 1945, so too now our dominance in IT and IW capabilities will confer a similar enduring dominance that will allow us to establish a Pax Americana and, presumably also deter any and all major threats.[3] Obviously they consciously employ the nuclear analogy when thinking about how to deter IW attacks.

Timothy Thomas of the U.S. Army's Foreign Military Studies office at Fort Leavenworth goes even farther and incorporates into his nuclear analogy Russian sources who see IW as a strategic threat comparable to nuclear weapons in their functional outcome.[4] As one Russian study of soldiers of the future concluded:

> *Ideologically these developments are based on the concept of an "information war", created on the basis of the latest achievements of scientific and technical progress and with an associated revolution in military science at the turn of he XXI century. By its consequences, it is possible to compare it only with the creation of nuclear weapons in the middle 1940s. The introduction of information-space technology at all levels of control and troop applications actually makes it possible to seriously speak about the possibility of "combat operations in digital form.*[5]

This Russian view has become an official one where Foreign Minister Igor Ivanov wrote to UN Secretary-General Kofi Annan to launch a process by which the UN could devise an international agreement to ban IW. Ivanov argued that IW's destructive potential was tantamount to that of strategic nuclear weapons and therefore it should be banned.[6] Most Russian writing on the subject points to the conclusion that Moscow would respond to an IW attack much as it would to a nuclear attack, i.e. by a nuclear counterattack.[7] And since its forces operate on a launch on warning basis, the confirmation of a threatened attack would serve to create great pressure for launching on warning or even preemptively.[8]

Richard Harknett presents the second opinion and argues that the potentials for using IT and IW to attack either the networks that bind societies together (netwar) or against more purely military targets (cyberwar) transcend the models of both nuclear and conventional deterrence and take us back to an earlier age where models of offensive and defensive strategies prevail.[9] In this connection netwar targets appear to resemble countervalue targets and cyberwar targets, counterforce targets. Precisely because IT binds together hitherto disparate social organizations, including the armed forces, into networks based on shared information and situational awareness, that connectivity can be attacked or contested. Because this connectivity can be targeted, it must be defended, or its enemy attacked. Therefore deterrence will be difficult, if not impossible. As he writes:

> *Information warfare is best understood by focusing on the concept of connectivity as both a societal and military asset. For strategists seeking to deter this new form of war, connectivity is a double-edged sword. Deterrence requires that the capability to inflict retaliatory costs be perceived as reliable. Deterrence weakens to the extent that the deterrent capability can be contested by a challenger through degradation or avoidance. The inherent accessibility of information technology invites challenges to a network's connectivity. Deterrent threats relying on such connectivity will be susceptible to technical, tactical, and operational contest. The contestability of connectivity will make deterrence of information warfare difficult.*[10]

Jargon aside, Harknett says that if the IT that makes the information systems that bind social and military networks together can be attacked, we must defend them or be able to attack enemies so that they cannot attack us. Or to use the terminology of nuclear deterrence, we must deter attacks on both counterforce and countervalue targets in future war. And since both sets of targets are so easily accessible, such deterrence is probably impossible for both categories of targets. For Harknett the past theology of deterrence is irrelevant. In an IW environment neither kind of target can be defended. Therefore we cannot deter attacks on them.

Whereas in the Cold War both sides came to realize that nuclear weapons were unusable because they achieved no true strategic advantage and only triggered an equally destructive second-strike, IT networks can be more easily attacked with greater chances of impunity. After all, an attack on an information network can, if sufficiently successful and comprehensive, make it impossible for the system to retaliate effectively. As Russians argue, a successful attack on an information network could inhibit the launching of a nuclear response or an equally destructive IW equivalent of the second strike.[11] Or it could so disrupt the governance of a state as to render it ungovernable. Furthermore, there is no mutually assured destruction. If one side's information capabilities are sufficiently degraded, presumably it cannot regroup and counter-attack. Nor can it then achieve the equivalent of launch under attack and have its IW capabilities, so to speak, in the air when the "bomb" lands. Information systems cannot take off or launch on warning or attack because if those systems are successfully attacked there is no warning capability left and because they can and probably will be attacked without warning.

Finally, former Secretary of Defense William Perry has argued for a third view that the new weapons systems that incorporate stealth, global and near-time reconnaissance capability, precision strike, and focused logistics will provide a more credible deterrent for theater-level conventional wars (not guerrilla wars) than nuclear forces. These systems should allow us to deter other conventional regional threats and regional challengers who might think of using chemical weapons.[12]

Presumably the advances in weapons technology since 1991 have further justified Perry and those who think like him in their outlook. Furthermore the synergistic combination of the new technologies and weapons capabilities that we alone can master will allow us to obtain what Perry calls "force dominance." Force dominance combines dominant maneuver, precision strike, forward basing, dominance of the air, focused logistics, and dominant battlespace awareness to such an extent that U.S. commanders will have "complete, real-time knowledge of the disposition of all enemy and friendly forces." But such knowledge will be denied to enemy commanders.[13] The "fog of war" will be dissipated and we will have complete knowledge. Thus our information systems can emerge relatively, if not totally, unscathed.[14]

Many writers attacked the notion of complete knowledge as fanciful and misguided, but it nevertheless became the official view during Perry's tenure in the Pentagon. It still enjoys great influence.[15] This view implies that in theater-level conflicts, the U.S. conventional superiority, much of which is embodied in information systems and IT, will allow us to detect, target, and deter others while remaining ourselves relatively undeterred and perhaps unseen.

In addition, since Perry first wrote on the new technologies in 1991, American military officials have sought ever more to incorporate the new systems into our military activities in peace operations and lower-level conflicts within the spectrum of conflict. Air Force officials like to claim that their bombing of Bosnian Serb targets in 1995 and our informational capabilities *alone* deterred the Serbs from further fighting and brought them to Dayton.[16] Since then it has become clear to U.S. officials monitoring the Dayton peace process that our public information and other information activities are equally strategic instruments of U.S. policy, elements of power that can shape the environment, resolve crises to prevent their escalation into conflict, deter future conflict, and be used for psychological operations.[17]

Thus our informational capabilities, as embodied in weapons, various communications media, reconnaissance capabilities, and information technologies like the Internet can supposedly shape the environment, prevent crises from exploding, and deter conventional conflicts across much of the spectrum of conflict. In other words, IT and the threat of IW can play the role of deterrent against other forms of military power. Since deterrence has always meant a willingness or even readiness to entertain the option of striking first with systems superior to those of the enemy (for example, our nuclear or high-tech weapons in response to his conventional systems), these same capabilities allow us to strike others first or even preemptively without warning.

Likewise, we are vulnerable to the same kinds of attack. Given the nature of international relations, our enemies will seek and in some cases find ways to deter our capabilities. We need only remember the words of Indian General Sundarji on the morrow of Operation Desert Storm who observed that the lesson was if you wish to fight the United States, you need nuclear weapons.

Indeed, this seems to be happening. North Korean, Iranian, Iraqi, and Chinese proliferation of WMD capabilities demonstrates that these states grasped Perry's message and will deter our capability by the threat of WMD, thereby diminishing or negating our advantage. Perry's policies are thus running into formidable resistance. The widespread efforts to acquire WMD capabilities represent conscious strategies to undermine the forward presence and technological superiority upon which our strategy depends.[18] The threat by Russia or some other enemy to use ballistic missiles or WMD also makes our allies' territory the battleground. Moreover, these states have repeatedly surprised our intelligence by their ability to enhance the qualitative and quantitative parameters of their systems or to use weapons of mass destruction in novel and truly strategic ways. We cannot complacently assume that we have and will have a decisive information superiority against them.[19] Furthermore, since we stress striking first, even preemptively, with conventional and informational weapons to degrade an opponent government's cohesion, no enemy will wait for us to end the war along with his ability to function. He will challenge us, probably preemptively, with weapons of mass destruction, low-intensity conflict, and information attacks to degrade our C4ISR, i.e. our center of gravity. Or an enemy will deploy besides his conventional forces other asymmetric threats that we do not handle well.

IW or asymmetric forms of war that are used preemptively against us because we threatened the enemy with similar attacks will unhinge our operational and strategic doctrines and surprise us. Repeated exercises and war games confirm this and show that we cannot count on a short war though our doctrinal templates tell us otherwise.[20] Those kinds of attack also seek to wrest control of the escalation ladder away from us and become even more likely where we confront an inferior conventional power. Simultaneously, the mutual race to preemption creates possibilities for threatening us or our allies because potential enemies fear being preemptively attacked, particularly if they are going for nuclear or other WMD capabilities. As Stephen Cimbala writes:

> *In other words, the revolution in military affairs could help to undo itself if it creates sufficient fears on the part of new [or old-SJB] nuclear nations that their capabilities will be subject to timely and decisive preemption whether or not they have threatened explicitly to use nuclear weapons against regional opponents.*[21]

Scholars studying the RMA and its impact on future war tend to agree that it provides the offense with many more means of victory, enhanced stealth, mobility, and capacity to concentrate precision fires without concentrating forces, and the ability to launch a preemptive strike against enemy C4ISR. When those factors are coupled with the stated U.S. strategy of launching a preemptive conventional strike, using precision-guided weapons and EW against enemies having a WMD capability, we find both sides racing to preempt and gain the offensive.[22] This race become particularly urgent in an environment where many believe that there will be only one uninterrupted strike or operation, so that whoever is attacked is already in trouble. Where only one side has futuristic weapons it may indeed gain the offensive, but where both sides have such capabilities or one side has nuclear weapons which it may use preemptively, or one side can "outflank" or preempt U.S. technological superiority, our offensive would face possibly insuperable obstacles.[23]

If both sides race to the offensive, the danger of war grows as does the danger of its prolongation beyond anyone's foresight or control. Deterrence becomes progressively more impossible to the degree that "players" lose control of the game. Since IW is the counter C4ISR weapon par excellence, it magnifies fears that one or both sides may lose control over their ultimate deterrents forcing them to use or lose them. Since either or both sides may lose control over their WMD or be unable to bring about an end to the conflict, IW may precipitate just what it seeks to avoid.[24] Thus if one side possesses a usable WMD capability and faces an IW threat that nullifies that capability, the latter becomes useless for deterrence and must be used preemptively to redress the balance.[25] Our enemies could then deter our IW by the threat of preemptive or first-strike ballistic missiles and/or WMD assault that may or may not be accompanied by IW, perhaps also used preemptively.

Both sides could then easily fall into the possibility of an escalatory spiral as each side tries to break out of the stalemate they have unwittingly created. The RMA works as prophesied when just one side has it. Otherwise it is highly unlikely that we can avoid either protracted or nuclear war in a major theater operation against an opponent with WMD capability. In fact, nobody can say for sure what war between two more or less RMA capable militaries would look like.

There are other points that favor Harknett's argument that he overlooked or did not consider. For example, analysts on both sides of the Atlantic agree that IW goes on in peace and in war.[26] Taken to an extreme, this means that we are in an information war right now. Even if we do not go this far, because we cannot be sure who the enemy is in an information war, the retaliatory threat implied in the theory of deterrence is greatly reduced in effectiveness. Moreover, if our own IT is successfully targeted our weapons of retaliation will certainly lose some of their effectiveness as deterrents. And because IW goes on constantly it also eliminates the distinction between peacetime and war which is essential to deterrence because states at whom the threat of retaliation is directed must be able to distinguish between war and peace and fashion a proportional response for deterrence to be effective.[27]

A second argument is that the resort to IW will eliminate any sense of early warning since those sensors may be among the first assets to be targeted. And because IW goes on in peacetime, it is all too likely—as past simulations suggest—that we will not know for sure if we were attacked by an enemy or a teenage hacker. Indeed, we may not even be sure that we were attacked. Similarly, if small state and non-state actors who have access to WMD and IW capabilities use them against us, deterrence will be a weak option. Thus our responses will be circumscribed and inhibited.[28]

There is a third political argument that Harknett overlooked when he observed that the recourse to IW will undermine deterrence. At present the United States and most other great powers are striving to develop cooperative security among themselves and cooperative, partner-like relations among themselves.

Such relationships depend upon confidence-building measures (CBM's) that provide enhanced transparency and more information to both sides. If the information provided is somehow unreliable or corrupted, the whole process is compromised. Then both sides may relapse into worst-case scenarios and unyielding mutual suspicion. Those perceptions of unreliability and suspicion make conflict all the more likely. If IW replaces CBM's as the normal peacetime mode of operation and transparency is rendered opaque or worse, then a valuable tool of early warning and mutual confidence is lost and escalation of IW attacks cannot be ruled out.[29] Under this logic, it would seem that the possibility of forfeiting trust and the risk of losing some EW capability does not deter the aggressor since he considers that the gain in degrading the enemy's capability or in deceiving him outweighs the risk. This argument also points to the conclusion that in many respects the resort to IW, even in peace, risks compromising foreign policy based on cooperative security that now appears to be a semi-universal goal.

A fourth overlooked argument is the fact that the revolution in military affairs (RMA) has so transformed the battlefield as to render the distinction between front and rear and between civilian and military targets moot.[30] Those conducting IW can and will target the civilian infrastructure as a way of striking at the sources of an enemy's military power and erase the distinction between counterforce and countervalue targets. That is not all. Conflating front and rear and civilian and military targets not only adds to the number of targets available, but also makes it almost impossible to deter adversaries from striking targets of value since anything may be attacked from anywhere and civilian and military targets become more nearly interchangeable. Indeed, the Pentagon talks of farming out more and more IW functions to civilians who thereby could be seen as combatants, thereby raising the possibility of a bloodier and even total war.[31]

As a final extension of this argument, Charles Dunlap raises a fifth point that Harknett overlooked. If information superiority is essential to victory, then the U.S. or other states will be driven to impose draconian measures against even non-belligerent purveyors of information, thereby running the risk of widening the war.[32] This tendency towards widening the war makes it difficult for both the attacked party and third parties not originally involved in the conflict to deter an attack against their vital infrastructures.[33]

Deterrence in an IW Context

In this section, we will determine the requirements of deterrence and measure them against attributes of IT and IW to determine if the arguments raised in support of Harknett's view are valid. Deterrence is a process of conscious mutual or bilateral interaction between states and armies over time. It is based as much on shared information and cognitive processes as anything else. If state A seeks to deter either a conventional or nuclear attack by state B it must make known much of its capability and resolve to deprive state B of victory (denial) or to impose such costs upon it as would make victory either meaningless or not worth the exertion involved (punishment).

For deterrence to succeed, State B must understand this communication for what it is. He must find it credible and understand it in terms of state A's frame of reference. He must thus grasp both State A's intention and capability and be able to weigh those facts against his own intentions and capabilities and calculate whether or not an attack is still worth pursuing. And he must be able to have a reliable channel of information and communication to, from, and about state A at all times.

Moreover, even if State A is a nuclear power, he must also realize that if State B has nuclear weapons or *may have them* that he may not be able to destroy B's capability even by a surprise attack or even by a second strike or in response to B's initial conventional attack. Thus he is himself vulnerable to a devastating riposte, i.e. mutually assured destruction.[34] This realization should limit war and even deter A or B from attacking each other since, even if the outcome cannot be determined, the consequences of attack at the nuclear level are extreme. Thus deterrence, if it works, should limit warfare and prevent it from going to the limit because that risks total destruction. As Martin Van Creveld has pointed out, wherever nuclear weapons have come to into the hands of states, major war between them has been ruled out.[35]

The same kind of reasoning applies as well to the cooperative security argument raised above. This is not surprising since the push for such a regime came out of a realization that deterrence could easily fail and lead to a dead-end or worse. Thus both sides needed to have ever more reliable information about each other's military programs, policies, capabilities, and doctrines. IW operations that corrode faith in the reliability of such information or make it impossible to know what is happening directly contradict the logic of such a political approach.

The provision of such information either under cooperative stability or a mutual deterrence regime should facilitate crisis stability since both side ultimately know or can reasonably estimate the thresholds beyond which they may not go. Furthermore one reason for the success of nuclear deterrence until now is the fact that we cannot predict or control the consequences of a nuclear strike. To the extent that national commands cannot gain reliable control over the course of a nuclear war or predict its outcome, that uncertainty has helped to deter nuclear war.[36]

Conventional deterrence, on the other hand, has often failed because states disregard, misinterpret, or do not understand the communications of resolve they are encountering. Or, as in the case of Egypt and Syria in 1973, they may calculate that launching a war, even if it ends badly operationally, has the strategic effect of forcing an alteration in the strategic and political status quo. Even states who are weaker than their opponents may attack believing that their capacity to make trouble will deter the stronger power for a time, if not give them victory.[37] Japan in 1941 approached that example. Since conventional deterrence may fail because of the failure of both sides to interpret the same data correctly, a technological difference divides it from nuclear deterrence.

Another argument on behalf of conventional deterrence states that it may be necessary to wage repeated if more limited wars to get aggressors to understand that they cannot win and therefore must gradually scale down their objectives.[38] We thus reach the strange sounding conclusion that if conventional deterrence is to succeed, not only must one or both sides be ready to wage war if attacked, either or both must actually do so repeatedly until one side learns its lesson. Given what we know about IW, if this notion were transferred to it, we would in fact say that in an IW world deterrence truly means incessant war.

Other issues are no less consequential. In nuclear cases, the technological capability of strategic nuclear weapons is so well-known that few governments are willing to cross the thresholds of nuclear use. Knowledge of those systems' capability is so reliable that it deters. It is the technological capability of strategic nuclear systems that has led to the well-known "nuclear taboo" in world politics with regard to use, not acquisition of those systems.

Clearly, the same does not hold true for conventional deterrence. This is either because the impact of the deterrer's going to war in response to aggression cannot be or is not always reliably assessed, or the assessment of potential costs is outweighed by an assessment of gains that can be made. Even the capability of high-tech weapons like IW systems may not be accurately estimated by adversaries in a crisis. Conversely, they may be willing to absorb that capability's impact to obtain other aims which are not readily apparent to the deterrer.[39]

It therefore seems that the quality or nature of the information available to would-be aggressors and to deterring states plays a critical role in making deterrence successful and/or viable. If reliable information about costs and risks is absent or unachievable, there evidently is a higher risk of a deterrence failure, just as Harknett suggested.[40] This observation returns us to our original insight about deterrence as a process of conscious interaction between states and armies over time where shared information and understanding is vital to success.

Thus we can postulate several requirements for effective deterrence. There must be clear and shared information, particularly about capabilities, the consequences of their use, and the resolve to use them whose significance is well appreciated by both sides. The communication of intention, capability, and resolve to deter must be equally clear and understandable by both sides according to their own or their mutual (if such exists) frame of reference. The national command authorities of nuclear powers should not be targeted because that is a wager on total war and invites a similar retaliation. Efforts to decapitate a national command and prevent it from maintaining control over its forces is also an attempt, not just at total war and total victory, but also to prevent any obstruction to one's plans or deterrence of them. Targeting those forces which can provide a state with reliable information pertaining to its adversary's deterrence capabilities, intentions, and resolve, surely signifies a determination not to be deterred even at the costs of total and unlimited war. Such targeting also precludes a surrender, a negotiated settlement, or possibly any settlement since the other side's ability to control the use of its nuclear weapons disappears with such an attack.

Such an attack attempts to undo what may be the single greatest deterrent of a nuclear strike, namely that nuclear war, we suspect, cannot be controlled. Therefore we do not want to free the genie from the bottle.[41] Precisely because we know that we do not know how to control that kind of war, we have been and are deterred. Yet precisely because IW is counter C4ISR warfare par excellence, the resort to IW almost compels a WMD armed opponent to strike first and preemptively or to follow Russia's example of a "dead hand" on the nuclear controls.[42]

The same cannot be said about conventional war. Hence we find in recent conventional conflicts beginning with *Operation Just Cause* in Panama deliberate targeting of the enemy's central government. Saddam Hussein followed suit in Kuwait, and Serbia did so in Sarajevo. The U.S. followed suit in Somalia and Haiti, and Russia did so in Chechnya. In all those cases the "offensive" side made clear its attempt to end one faction's or ruler's tenure in office and install a more pliable regime. Such a war could not be limited for the government under attack for if it lost, it was out or dead, or both. But had those embattled regimes or factions had nuclear deterrents, that capability would very likely have been communicated to its enemy and forced a reconsideration of policy. Thus many recent conflicts, despite self-proclaimed adherence to limited war, actually were or became total wars where the survival of a regime was the issue at stake.

Clearly, where the state bent on destroying the other side's capacity to govern itself is vastly superior technologically, it cannot be easily deterred, if at all. The launching of a war under those conditions or the threat of doing so will lead the embattled government either to launch its own preemptive IW strike or to adopt an unconventional and protracted war strategy which requires little in the way of the high-tech that the U.S.

must have. This nullifies many of advantages. Moreover, as in Mexico's Zapatista wars or other such insurgencies, the underdog may have access to global information sources that mitigate his inferiority. Thus he may not be able to deter the superior force, but that force may not be able to fight the kind of war it prefers.

Other Factors

Similarly, in the Middle East we have already seen the resort to WMD since 1962 when Egypt used chemical war with impunity in the Yemeni civil war. In the 1980s, Iraq used missile and chemical strikes against Iran to positive strategic effect, perhaps for the first time in modern war. Iraq was not censured at the time by anyone. Sanctions emerged in response to the invasion of Kuwait, not the war of 1980-88.[43] Other actors might be inspired to imitate Iraq in the belief that they can use such weapons as effective countervalue or counterforce systems. Given the findings of the Rumsfeld Commission that we may not have prior notice of such capabilities through tests because these states may not feel the need to test their systems, we or our allies could be blindsided.[44] This possibility excludes the likelihood of being deceived or of suffering intelligence failures, things with are pervasive throughout military history.

IW works against deterrence in other ways as well. In deterrence situations, both sides must have the necessary time to receive these signals of capability and intention from their adversary and to grasp their import. In nuclear scenarios they must share the same sense of uncertainty concerning weapons of mass destruction and have an essential monopoly over them to maintain control over the processes by which crises might escalate out of control. They must be able to distinguish attacks from accidents or unauthorized actions, a capability which also depends on early warning, time to assimilate information, and time to act correctly upon it. All these requirements also contain as a prerequisite functioning and verifiable mechanisms of communication between the two states so that they can send each other clear and reliable information about each other's policy and the nature of the threat.[45]

Time is essential for both sides in a conventional deterrence relationship if they truly mean to deter and can be deterred. However, it is not enough if one of them means to attack, particularly if they cannot correctly understand or will not try to grasp the meaning of the signals coming from the external environment. In fact, under such conditions, attempts to initiate a bilateral process of communication may make the ensuing attack all the more devastating and surprising. Stalin refused to believe up to the end that an attack was imminent. Hence the attack, when it did come, was even greater than might otherwise have been the case. U.S. leaders, though knowing of an attack from Japan, failed to understand its imminence or location and were utterly surprised in 1941. Israel in 1973 was put off balance by repeated crises and maneuvers that ended short of war and led Jerusalem to think that the Arabs were deterred. Saddam Hussein had six months to withdraw from Kuwait but disregarded or misunderstood American conventional deterrence. (Interestingly, he did not disregard nuclear deterrence and launched no chemical or biological attacks on the allies or Israel, presumably because he knew the consequences that had been publicly spelled out of doing so.) The list of conventional failures hardly ends there.

There must also be a kind of strategic symmetry between the two states (and they do not have to be the USA and USSR in the cold war). Each state must have sufficient capability to do serious damage to the other either conventionally or strategically. Thus while the Soviets could destroy Europe after 1945, the United States could then have destroyed the USSR. That was the essential condition of early postwar deterrence. Later, when Moscow attained nuclear parity, the two blocs' relationship became codified as a mutual hostage relationship since they could destroy each other. But whereas nuclear capabilities soon became clear to both sides, conventional deterrence failures, even where weaker powers launch asymmetric attacks on stronger states, suggest that information about relative capabilities, intentions, and resolve, is much easier to disregard or misinterpret.

What seems clear is that deterrence can only work when four conditions apply. First, both sides must have access to similarly (or relatively similarly) understood data about each side's intentions, capabilities, and resolve. Second, both sides must have time to make the right assessment. Third, both sides must appreciate that they each stand to lose something of comparable if not equal value from a deterrence failure and may gain little or nothing. Finally, both sides' ability to communicate with their own systems and each other must remain reliable and relatively unimpaired so that they can maintain control over the crisis and accurately evaluate incoming information. Thus, for deterrence to work effectively, neither side's informational capabilities can be impaired or compromised.

Information Warfare and Deterrence

From the foregoing it is clear that successful deterrence can not occur in the absence of reliable and verifiable information networks and communications mechanisms on both sides. But IW may put precisely those critical aspects of deterrence into question. We must not define information warfare as strictly limited to attacks by either computer based technologies against military targets or information networks on the other side. Logic bombs, viruses, and so on do not exhaust the repertoire of IW. Soviet and Russian writers got it right when they observed that the new weapons coming on stream possess both an information and a strike component. The former consists of the reconnaissance component. It selects the target's location and allows for stealth or evasion of defensive systems while the strike component hits the target. Thus information warfare consists of attacks against information networks and against the informational component of weapons systems. This definition expands the scope of IW, but forces us to realize that there are other definitions besides ours. Thus, if we go a step farther along this line of logic, it becomes clear that one way to deter a state with a "reconnaissance—strike capability"—IW and high-tech combined together—is to strike at its sensors, e.g. anti-satellite warfare which could be profoundly destabilizing.[46]

The point here is that IW is almost by definition counter-command and control warfare and strikes at those relationships and mechanisms that make deterrence possible and effective. If deterrence between WMD powers is to be effective where one or the other has IW capabilities, those capabilities must be reined in lest they undermine deterrence and unleash an uncontrolled and uncontrollable war.

IW capability is by nature elusive and has an almost undefinable capability. Governments possessing this capability seek to protect their utility by not advertising their full potential, unlike they do with other systems. They also cannot know what the full ramifications of IW strikes on another society are because they would not necessarily be striking at a tangible, visible, or measurable capability. It seems almost impossible to model mathematically what the impact would be of shutting down Wall Street or a national electric grid. Nor is it a simple matter to know that if you can reliably shut down an enemy's C4ISR capability that you get victory. Certainly this is not true with regard to Russian nuclear missiles which apparently have a doomsday capability.[47] They may even have a pre-delegation capability distributed to their commanders which would allow them to launch if central command was compromised. The same may be true for other nuclear powers.

But where we had warning time, even if only minutes, in nuclear or theater conventional scenarios, in an IW scenario we can be attacked by anyone from anywhere at any time. We may not even know we were attacked. In many cases, we will correctly evaluate the information we receive, either because it is corrupted by an IW attack, incomplete, or inconclusive in that we cannot reliably conclude who attacked us or why we were attacked. For instance, a RAND Corporation game found that we lacked adequate tactical warning of cyber attacks and the ability to identify who the enemy was. It also found that those playing the game could not agree on whether they were attacked or whether such attacks constituted an act of war. Nor could those playing find out if the attacks were the limit of an enemy's capability. Many players were frustrated by the lack of strategic intelligence—a prime example of friction and fog that directly refuted the confident forecasts of those writers who assume near perfect knowledge—which "crippled the administration's capacity to take decisive action."[48]

This last point adds another aspect to the mix. Whereas deterrence, to be effective, must rely on accurately conveyed information and *understanding* of that data, IW aims precisely to undermine confidence in any data or to give one a false picture of the real world, or to deprive an enemy of the capability of making informed strategic judgments. IW's purpose is to take the ability to make accurate decisions about our or our enemy's forces out of his or our hands. The ambition of an information warrior is precisely to make this essential precondition of reliable deterrence unusable or unreliable. And since it occurs in peace and war, it is inherently a double edged sword. On the one hand, an armed force or government can use IW to make clear to an opponent the awful retribution that will be visited upon him if he attacks. On the other hand, it could be used even in peacetime as part of a pattern to disorient or mislead him.

In a conflict scenario, given our stated ambition of depriving our enemy of the capability of autonomous self-government, we are inviting a preemptive strike which, if successful, will make it all but impossible for us to react. While the explosion of information could lead to more open networks and greater mutual understanding even between enemies, the race to degrade enemy information capabilities suggests that IW has unique properties unlike conventional or nuclear war and unlike their deterrence models.

Conclusions

IW attacks may have functional and strategic, but not physical, outcomes comparable to nuclear ones, as Thomas, the Russians, and Owens and Nye contend. Like conventional and nuclear attacks, information retaliation may include private sector targets with extensive collateral damage outside of the actual battlefield. But Harknett's approach seems more compelling except in one case, where a government has a WMD capability that it is ready to use preemptively to deter an IW attack. For instance, because it is hard to identify the origin and identity of attacking forces, proportional retaliation in kind against IW attacks is difficult. The more one depends on a degraded information capability to initiate retaliation, the harder it becomes to retaliate. While we can distinguish between conventional and nuclear attacks, IW may be a seamless process that begins as a small episode and escalates to large attacks with effects comparable even to nuclear attacks.[49]

The foregoing suggests that IW cannot be deterred by another IW force since both sides can deceive or cripple an opponent's ability to make the kind of evaluations upon which deterrence depends. Preemptive IW becomes a viable, even almost necessary option. Since everyone has access or will have access to forms of IW and can use commercially available satellites, cell phones, PC's, and the like to launch delayed attacks, hack systems, and so on, IW deterrence must be ubiquitous and universal to be effective. Otherwise the temptation to strike first can be overwhelming.

This trend towards defending everything can be seen in the U.S.' accelerated efforts to set up homeland and anti-terrorist defense organizations. But evidence suggests that despite our technological superiority we cannot accurately deter or predict what enemy forces will do, especially when they target our insight into their thought processes or vice versa.[50] Nor is it clear that we can deter our adversaries if our strategy focuses on destroying their ability to command troops, govern the country, and control WMD.

Neither is it clear that overwhelming conventional force can deter IW. Conventional deterrence could be preempted by an IW attack which grounds those forces or diverts their attention, to create a domestic crisis. Furthermore, few states will try to fight the U.S. where it is strongest and least vulnerable—high-tech precision conventional systems. As many have pointed out, the greater risk is the use of asymmetrical means, perhaps even combining some elements of IW, WMD, missiles, and unconventional war.[51] This may explain why those states that might contend with the United States or with other major conventional powers—China, Russia, India, Iran, Iraq, Israel, Pakistan, and North Korea—are developing WMD capabilities. Fearing a U.S. or other powers' major attack, these states may move to preempt us and other enemies by deploying such capabilities. That might inhibit our allies from letting us use their territories as forward staging bases and undo our basic strategy of forward presence.[52]

This essay suggests that neither our models of conventional or nuclear deterrence can deter an IW attack except where an opponent has a usable WMD capability. IW threats apparently even add incentives for using WMD, conventional, and IW weapons immediately, even preemptively, lest they be otherwise lost in the first and possibly only strike. The threat of such preemptive strikes may well deter even other nuclear and conventionally and informationally superior states from attacking each other's vital interests. But this does not mean that states will not fight for their vital interests against what they believe are less important interests of major powers. Hence IW, like nuclear weapons, has made the world safe for conventional war.[53]

But if WMD in the hands of our enemies are the only ways they have to deter us, they will acquire those capabilities and as many of the high-tech conventional and IW capabilities that we have to deter us and be able to wage conventional war for their own objectives. In short, we may not be able to move beyond an IW arms race while remaining shackled at the same time by the proliferation of weapons of mass destruction. For those who triumphantly hail a new dawn based on the enduring superiority of American military power, this is a sobering, if not depressing observation. But it would not be the first time that inventions that supposedly made war shorter and more humane, actually made the nightmare all too real and converted this supposed sunrise of hope into one more false dawn.[54]

[1] Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *Proceedings of the U.S. Naval Institute* (January, 1999), p. 36; Bob Herbert, "War Games," *New York Times*, February 23, 1998, p. E17; Ralph Peters, "Spotting the Losers: Seven Signs of Non-competitive States," *Parameters*, XXVIII, No. 1 (Spring, 1998), p. 36; George and Meredith Friedman, *The Future of War; Power, Technology and American World Dominance in the Twenty-First Century* (New York: St. Martin's Griffin, 1998). The final title spells out the prevailing mood. This insight is also based on playing the U.S. Army War

College's annual Strategic Crisis Exercise from 1995-98 and the Army After Next Spring game in 1998 where coalition formation and maintenance invariably broke down or was often not even seriously attempted by the uniformed U.S. military. See also Michael Brenner, "The United States," Michael Brenner, Ed., *NATO and Collective Security* (New York: St. Martin's Press, 1997), pp. 162-175.

[2] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown & Co. Inc., 1993), p. 84.

[3] Admiral William T. Owens and Joseph Nye, "America's Information Edge," *Foreign Affairs*, (March-April, 1996), pp. 20-36.

[4] Lester W. Grau and Timothy L. Thomas, "A Russian View of Future War: Theory and Direction," *Journal of Slavic Military Studies*, (September, 1996), pp. 501-518; Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters*, (Winter, 1996-97), pp. 81-91; Timothy L. Thomas, "Russian Views on Information-Based Warfare," *Airpower Journal*, (Special Issue, 1996), pp. 25-35; and Timothy L. Thomas, "Dialectical Versus Empirical Thinking: The Key elements of the Russian Understanding of Information Operations," Paper Presented to the U.S. Army War College, Annual Strategy Conference, April 22-24, 1997, Carlisle Barracks, Pa. See also Edward Waitz, The U.S. Transition to Information Warfare," *Journal of Electronic Defense*, (December, 1998), p. 36; and Sergei Modestov, "The Possibilities for Mutual Deterrence: A Russian View," *Parameters*, (Winter, 1996-1997), pp. 92-98.

[5] V. Men'vikov, I. Golovanev, and S. Pavlov, *Soldiers of the Future,* National Air Intelligence Center, July, 1997*,* p. 3.

[6] Matthew Campbell, "'Logic Bomb' Arms Race Panics Russia," *The Sunday Times (London)*, November 29, 1998.

[7] Stephen Blank, "Nuclear Strategy and Nuclear Proliferation in Russian Strategy," *Report of the Commission to Assess the Ballistic Missile Threat to the United States*, Appendix III, Unclassified Working Papers, Pursuant to Public Law 201, 1998, pp. 57-77. See also "Proliferation and Counterproliferation in Russian Strategy," presented to the JINSA-SSI Conference on Proliferation Strategies, Washingto,D.C. February 22, 1999.

[8] *Ibid.*

[9] Richard Harknett, "Information Warfare and Deterrence," *Parameters*, (Autumn, 1996), pp. 93-107. See also his other article, "The Logic of Conventional Deterrence and the End of the Cold War," *Security Studies*, (Autumn, 1994), pp. 86-114.

[10] Harknett, "Information Warfare and Deterrence," p. 93.

[11] Blank, *Ops. Cits*., and Thomas, *Ops. Cits*.

[12]"The Information Edge: America's Non-Nuclear Deterrent," An Interview with Former Secretary of Defense William Perry, *New Perspectives Quarterly*, (June, 1997), p. 45. William J. Perry, "Desert Storm and Deterrence," *Foreign Affairs*, (October-December 1991), pp. 66-82, and idem.,"Defense in an Age of Hope," *Ibid.*, LXXV, No. 6, 1996, pp. 64-79.

[13]As Thomas Behling and Kenneth McGruther observe, our strategic formulations presume virtually perfect knowledge and unimpeded satellite and sensor transmissions. Thomas G. Behling and Kenneth McGruther, "Satellite Reconnaissance of the Future," *Joint Forces Quarterly*, (Spring, 1998), p. 24. For other sources that represent this view, see General Ronald R. Fogelman, USAF, "The Air Force and Joint Vision 2010," *Joint Forces Quarterly*, (Winter, 1996-1997), p. 25; Major General Charles Wald, USAF, "Air Force Next: The High-Tech Force," Briefing to the Defense Science Board, February 4, 1998, p. 2; National Military Strategy of the United States, 1997 located at www.dtic.mil/jcs/nms/executiv.htm (Henceforth NMS); General John M. Shalikashvili, *Joint Vision 2010*, (Washington, DC: USGPO, 1997); Joint Chiefs of Staff, *Concept for Future Joint Operations: Expanding Joint Vision 2010*, (Washington, DC 1997); *Report of the Quadrennial Defense Review*, (Washington, DC, 1997), pp. 39-42 (Henceforth QDR); Benjamin S. Lambeth, "The Technology Revolution in Air Warfare," *Survival*, (Spring, 1997), pp. 65-83; Col. Richard Szafranski, USAF, "Parallel War: Promise, Problems," *Proceedings of the U.S. Naval Institute*, (August, 1995), pp. 57-61; Harlan K. Ullman, James P. Wade, et al., *Shock and Awe: Achieving Rapid Dominance* (Washington, DC: The Center for Advanced Concepts and Technology, National Defense University Press, 1996); Daniel Goure and Stephen A. Cambone, "The Coming of Age of Air and Space Power," Daniel Goure and Christopher M. Szara, Eds., *Air and Space Power in the New Millennium*, (Washington, DC: Center for Strategic and International Studies, 1997), pp. 1-47; Alvin H. Bernstein and Martin Libicki, "High-Tech: The Future of War?," *Commentary*, (January, 1998), pp. 28-31; *TRADOC Pamphlet 525-5 Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations in the Strategic Army of the Early Twenty-First Century*, (August, 1994); Headquarters, Department of the Army, *FM 100-6: Information Operations*, (August, 1996); Stuart E. Johnson and Martin C. Libicki, Eds., *Dominant Battlespace Knowledge*, (Washington, DC: Institute for National Security Studies, National Defense University Press, 1995); "Brass Hats Get Down to Brass Tacks," *The Guardian*, May 24, 1997; Dean A. Nowowiejski, *Concepts of Information Warfare in Practice: General George S. Patton and the Third Army Information Service*, (Ft. Belvoir, VA.: Defense Technical Information Center, 1996), pp. 2-3; Admiral William Owens, "Foreword," Stuart J.D. Schwarzstein, Ed., *The Information Revolution and National Security: Dimensions and Directions*, (Washington, DC: Center for Strategic and International Studies, 1996), p. xii.

[14] *Ibid*.

[15] *Ibid.* The most powerful and, in the author's view correct, refutation of the view that we will eliminate the fog of war is Barry D. Watts, *Clausewitzian Friction and Future War*, (Washington, DC: Institute for National Security Studies, National Defense University, McNair Paper No. 52, 1996).

[16] This was particularly evident from the speeches by Air Force leaders at the Dueling Doctrines Conference, Washington, DC June 24-25, 1998.

[17] Pascalle Combelles Siegel, *Target Bosnia: Integrating Information in Peace Operations*, (Washington, DC Institute for National Security Studies, National Defense University, 1998), pp. 67, 85.

[18] For a comprehensive study of all these activities, see *Report of the Commission to Assess the Ballistic Missile Threat to the United States*, Appendix III, Unclassified Working Papers, Pursuant to Public Law 201, 1998.

[19] *Ibid*.; Robert David Steele, "Private Enterprise Intelligence: Its Potential Contribution to National Security," *Intelligence and National Security*, (October, 1995), pp. 214-216; Abraham Ben-Zvi, "The Dynamics of Surprise: The Defender's Perspective," *Intelligence and National Security*, (October, 1997), pp. 113-144.

[20] Pat Cooper, "War Game Predicts Challenging, Lengthy Future Conflicts," *Defense News*, December 2-8, 1996, p. 31.

[21] Stephen J. Cimbala, "Russia's Nuclear Drawdown: Justice Delayed or Denied?" *European Security*, (Autumn, 1997), p. 81. To confirm the rightness of these fears cited by Cimbala, see General Ronald R. Fogelman, "Theater Ballistic Missile Defense," *Joint Forces Quarterly*, (Autumn, 1995), p. 76. Since Fogelman was then Chief of Staff of the Air Force, his discussion could be taken for accurately reflecting at least the Air force's strategic preoccupations and intentions.

[22] John Orme, "The Utility of Force in a World of Scarcity," *International Security*, (Winter, 1997/98), pp. 150-155.

[23] *Ibid*., pp. 155-156.

[24] Walter Slocombe, "Preplanned Operations," in Ashton B. Carter, John D. Steinbruner, and Charles A./Zraket, Eds., *Managing Nuclear Operations*, (Washington, DC: The Brookings Institution, 1987), pp. 121-141, is only one of many essays in this and other volumes that insist upon the centrality of command and control of nuclear forces.

[25] *Ibid*.

[26] Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace…the Decisive Edge in War*, (Washington, 1996), pp. 4-6; *Armeyskiy Sbornik (Moscow)*, September, 1996, FBIS-UMA-96-241-S, September 1, 1996; and Col. E.G. Korotchenko, "Informatsionno-Psikhologicheskoe Protivoborstvo v Sovremennykh Usloviakh," *Voennaya Mysl'*, (January-February, 1996), pp. 22-28.

[27] Waitz, p. 36.

[28] Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, (Santa Monica, Ca.: Rand Corporation, 1996), pp. 19-33, Commander John Richardson, "Strategic Thinking in an Era of Intervention: Thinking Out of a Box With No Sides," *Comparative Strategy*, (January 1999), p. 32, Douglas C. Lovelace, Jr., *The Evolution in Military Affairs: Shaping the Future U.S. Armed Forces*, (Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 1997), p. 33.

[29] Vladimir Petrovsky, "Transparency and Confidence-Building in the Asia-Pacific Region," *Far Eastern Affairs* (No. 5, 1998), p. 4.

[30] David S. Alberts, *The Unintended Consequences of Information Age Technologies*, (Washington, DC: The Center for Advanced Concepts and Technology, Institute of National Security Studies, National Defense University, January, 1998), pp. 3-5; and Gebhard Geiger, "International Security in the Information Age: New Structures and Challenges,“ *Aussenpolitik*, (No. 4, 1997), pp. 404-405.

[31] Col. Charles J. Dunlap Jr., USAF, *Technology and the 21st Century Battlefield: Recomplicating Moral Life for the Statesman and the Soldier*, (Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 1999), pp. 12-16.

[32] *Ibid*., pp. 21-22.

[33] *Ibid*.

[34] For an example of the need for such intra-war regimes and deterrence even during a limited nuclear war, see Paul Bracken, "War Termination," in Carter, Steinbruner, and Zraket, Eds., pp. 202-204.

[35] Martin Van Creveld, *Nuclear Proliferation and the Future of Conflict*, (New York: The Free Press, 1993), passim.

[36] Stephen J. Cimbala, *Military Persuasion: Deterrence and Provocation in Crisis and War*, (University Park, Pa.: Penn State University Press, 1994).

[37] T.V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers*, (Cambridge: Cambridge University Press, 1994).

[38] Uri Bar-Joseph, "Variations on a Theme: the Conceptualization of Deterrence in Israeli Strategic Thinking," *Security Studies*, (Spring, 1998), pp. 145-181.

[39] Paul, passim.

[40] Harknett, Ops. Cits., See also Peter Feaver, "Blowback: Information Warfare and the Dynamics of Coercion," *Security Studies*, (No. 4, 1998), pp. 88-120, on the importance of accurate information to deterrence.

[41] Slocombe, pp. 121-142; and Bracken, pp. 199-204.

[42] *Pravda Pyat*, January 30-February 6, 1998, in *Foreign Broadcast Information Service Central Eurasia* (Henceforth FBIS SOV), 98-084, March 25, 1998, Moscow; *Segodnya*, February 5, 1998, in *FBIS-UMA-98-036*, February 5, 1998; David Hoffman, "Decline of Russia's Nuclear Forces," *Washington Post*, March 15, 1998, p. 1; Bruce Blair, *The Logic of Accidental Nuclear War*, (Washington, DC: Brookings Institution Press, 1993), and Idem., *Global Zero Alert for Nuclear Forces*, (Washington, DC: (Brookings Institution Press, 1995), pp. 18-23, 43-72. See also his interview with John Newhouse, *Europe Adrift*, (New York, Pantheon Books, 1997), pp. 211-212; and Peter Pry's unpublished manuscript *War Scare*.

[43] Timothy D. Hoyt, "Diffusion From the Periphery: The Impact of Technological and Conceptual Innovation," Paper Presented to the 40th Annual Convention of the International Studies Association, Washington, DC, February 18, 1999.

[44] "Executive Summary of the Report of the Commission to Assess the Ballistic Missile Threat to the United States," July 15, 1998, Pursuant to Public Law 201, 104th Congress, *Report of the Commission to Assess the Ballistic Missile Threat to the United States*, Appendix III, Unclassified Working Papers, Pursuant to Public Law 201, 1998.

[45] Bracken, pp. 202-204, Paul B. Stares, "Nuclear Operations and Antisatellites," *Ibid*., pp. 679-702.

[46] Blair, Ops. Cits.

[47] Molander, Riddile, and Wilson, pp. 19-33.

[48] Waitz, p. 36.

[49] "Executive Summary of the Report of the Commission to Assess the Ballistic Missile Threat to the United States," July 15, 1998, Pursuant to Public Law 201, 104th Congress, *Report of the Commission to Assess the Ballistic Missile Threat to the United States*, Appendix III, Unclassified Working Papers, Pursuant to Public Law 201, 1998.

[50] For a revealing sign of the debate on this topic see *Summary Report From the Conference on Preparing Now: Alternative Paths to Military Capabilities for an Uncertain Future*, (Cambridge, MA: Institute for Foreign Policy Analysis, 1998), and the remarks of Captain James FitzSimonds, USN, in "Beyond the Technological Frontiers of Force XXI," *Final Proceedings of an Army After Next Project Conference*, (Atlanta, GA: Georgia Institute of Technology, Center for International Strategy, Technology, and Policy, 1996), pp. 9-10.

[51] For an extended discussion of the issues involved in extended deterrence and proliferation see Charles T. Allan, "Extended Conventional Deterrence: In From the Cold and Out of the Nuclear Fire?," *Washington Quarterly*, (Autumn, 1994), pp. 201-233.

[52] Lieutenant Commander Jeremy Stocker, Royal Naval Reserve, "Nonintervention: Limited Operations in the Littoral Environment," *Naval War College Review*, (Autumn, 1998), pp. 56-59.

[53] Van Creveld, passim. As Paul Bracken wrote in 1987, "Central to the theory of limited nuclear war and termination is the ability of U.S. military forces to meet an opponent on several levels of conflict." See Bracken, p. 199.

[54] Dunlap, pp. 1-3.

CHAPTER 5

MILITARY STRATEGY AND INFORMATION TECHNOLOGY:

ALTERNATIVE VISIONS OF FUTURE WAR

By
Steven Metz

The defining feature of our time is not the amount of information available or the pervasiveness of technology, but the pace and extent of change. Today all dimensions of life—social, personal, economic, political, ethical—shift rapidly. Transformation and revolution are daily undertakings rather than rare episodes. “By almost any measure,” writes Hans Moravec, “the developed world is growing more capable and complex faster than ever before.”[1] The sheer velocity of modern life creates new schisms and conflicts. Individuals and organizations able to adapt to the pace of change and at times even control it prosper. Those that cannot experience anxiety, dysfunction, stress, conflict, and failure.

This maelstrom of change is having a major impact on warfare and military organizations. The consensus among military analysts is that the world is in the midst of an historic transformation of war. The notion of a “revolution in military affairs,” which first entered the lexicon of Western thinkers a decade ago or less, is now an article of faith. All know that technology, particularly information technology, is the locomotive of this revolution, but there is little agreement beyond that. The information age is leading us somewhere at a breakneck pace, but we do not know where.

Despite intense analysis over the past few years, it is not clear how the Information Revolution affects the conduct of warfare. Will it simply be like other genres of technology, giving advantages to advanced militaries who develop, apply, and integrate it? Or will it transform the conduct and purpose of warfare in some fundamental way, altering basic power balances and relationships? Within the American strategic community, a series of visions of the future have taken shape, each of which answers these questions in some way. Some overlap and some are mutually exclusive. They range from the conservative to the radical. Because they deal with the future, these alternative visions are often conceptual, speculative, and abstract. No one knows what technology will allow in 20 years. More importantly, no one knows how humans will react to or use new technology. These alternative visions of future war are not purely academic. Decisions and assumptions made today about the future of warfare will shape the U.S. military of the new century. Americans must thus carefully scrutinize the official vision, assess its adequacy, and, if it is held to be flawed, decide which alternative trajectory the nation should select. Choosing incorrectly today could set the U.S. on the path to danger, perhaps even disaster.

The Official Vision

The Pentagon's official concept of future war expects emerging technology, especially information technology, to have a substantial impact on the conduct of military operations, but combines this with a conservative strategic perspective. States and their militaries are expected to remain the most significant actors. Armed conflict will remain an extension of policy. It will continue to be organized into discrete wars, campaigns and operations. Within the Department of Defense and the services, the vast majority of futures studies, war games, and exercises entail unambiguous cross-border aggression or the threat of such aggression by another nation state, sometimes a regional "rogue state," sometimes a "near peer competitor." The aggressor seeks to conquer neighboring states in which the United States has an economic interest (often petroleum). The U.S. military is able to use qualitative advantages to deter aggression, preempt an invasion, or turn it back once it occurs. These future wars are much like Desert Storm or what planners think that a NATO-Warsaw Pact war might have been like, but with an appliqué of new technology, new operating environments (cyberspace and orbital space), and moderate change in the structure of military organizations, whether the divisions, brigades, and battalions of the Army and Marines, the Air Force's wings and squadrons, or the Navy's task forces and air squadrons.

"Information superiority" will be the key to American battlefield success in the official vision of the future. Deriving from a "system of systems" that connects space-based, ground-based, and air-based sensors and decision-assistance technology, information superiority will allow American commanders to use precision weapons, many fired from safe locations far from the battlefield, to strike the enemy's decisive points at exactly the right time. To a large extent, American forces will be omniscient while enemy forces are confused and blind.[2]

The most comprehensive expression of this official vision is *Joint Vision 2010*, issued by General John M. Shalikashvili when he was Chairman of the Joint Chiefs of Staff. Known as *JV 2010*, this is the conceptual template for the future U.S. military. It seeks a force which can attain "full spectrum dominance," meaning that it is qualitatively superior to any anticipated enemy. *JV 2010* focuses on a state enemy using combined arms warfare against a neighbor. This enemy will be advanced but qualitatively inferior to the U.S. in key technologies. The key to success in an increasingly lethal battlespace will be "dominant battlespace awareness" growing from the system of systems. *JV 2010* states:

> To cope with more lethal systems and improved targeting, our forces will require stealth and other means of passive protection, along with mobility superior to the enemy's ability to retarget or react or our forces. Increased stealth will reduce an enemy's ability to target our forces. Increased dispersion and mobility are possible offensively because each platform or individual warfighter carries higher lethality and has greater reach. Defensively, dispersion and higher tempo complicate enemy targeting and reduce the effectiveness of area attack and area denial weaponry such as weapons of mass destruction (WMD). The capability to control the tempo of operations and, if necessary, sustain a tempo faster than the

enemy's will also help enable our forces to seize and maintain the initiative during military operations.[3]

The JV 2010 force will gradually abandon old ideas like massed forces and sequential operations in favor of massed effects and simultaneous operations. These will be possible because information technology will allow commanders to identify targets and coordinate complex actions much better than in the past. Technological advances, according to JV 2010, "will continue the trend toward improved precision. Global positioning systems, high-energy research, electromagnetic technology, and enhanced stand-off capabilities will provide increased accuracy and a wider range of delivery options."[4]

To make maximum use of the potential of new technology, *JV 2010* outlines four "new operational concepts" that are to guide the development of the U.S. military and military strategy. These include: *dominant maneuver*, defined as "the multidimensional application of information, engagement, and mobility capabilities to position and employ widely dispersed joint air, land, sea, and space forces to accomplish the assigned operational tasks"; *precision engagement,* which will allow very accurate aerial delivery of weapons, discriminate weapon strikes, and precise, all-weather stand-off capability from extended range; *full-dimensional protection* of American forces based on active measures such as battlespace control operations to guarantee air, sea, space, and information superiority, and integrated, in-depth theater air and missile defense, and passive measures such as operational dispersion, stealth, and improved sensors to allow greater warning against attack, including chemical or biological attack; and *focused* *logistics* which is "the fusion of information, logistics, and transportation technologies to provide rapid crisis response, to track and shift assets even while enroute, and to deliver tailored logistics packages and sustainment directly at the strategic, operational, and tactical levels of operations."[5]

Joint Vision 2010 was intended to synchronize the independent futures programs which the services had begun to develop. Where *JV 2010*'s time frame was mid-term and its intent was to provide a conceptual template, the Joint Experimentation Program created at the United States Atlantic Command (USACOM) in 1998 sought to expand the U.S. military's thinking about future warfare by weaving together the services' futures programs.[6] This is an ambitious undertaking. Futures-oriented thinking deals with force development, which is primarily a function of the military services rather than the Joint Staff or unified commands. Since the services have seen a long-term erosion of their prerogatives in favor of the Joint Staff and unified commands, they are likely to cling tenaciously to their futures programs. In fact, the Army, the Air Force, and Sea Services have each developed a range of futures programs based on their expectation about the future security environment and the future of war.

The Army has done the most in this arena. In fact, few large institutions anywhere have thought more about the future than the U.S. Army. Since there is no White House, National Security Council, or congressional concept of the future security environment or long-term American national security strategy, the Army has crafted its vision of the future and the role of landpower on its own. It has formulated a vision that is highly innovative in its approach to technology, organization, and leadership, but conservative in its assumptions about the nature of warfare and the purposes of power.

This blend of innovation and conservatism runs throughout the documents and programs that explain the Army's view of the future.

Army Vision 2010 outlines how the Army will support the ideas introduced in *Joint Vision 2010*. It contends that landpower will remain the most salient form of military power in the future security environment. This is because many military activities will occur on the lower and middle portions of the continuum of military operations, because most foreign militaries will remain landpower oriented, and because landpower makes permanent "the otherwise transitory advantages achieved by air and naval forces."[7] *Army Vision 2010* argues that the Army is best suited among the services to deal with asymmetric challenges such as urban combat, terrorism, information warfare, and insurgency. While it notes that operations other than full-scale war will be the most common task of the 21st century Army, it identifies the possibility of conventional war against "once dominant states [which] perceive an unfavorable shift in power relative to their neighbors." Oil and "radical fundamentalism," according to *Army Vision 2010*, might motivate war in the "Euro-Middle East region," while a shortage of food and arable land might do likewise in "the Asian arc." Should this occur, the Army might be called on to defend or liberate territory, contain a conflict, or undertake other missions.[8]

To transform the concepts outlined in documents like *Army Vision 2010* into reality, the Army has developed a series of simulations and exercises called Louisiana Maneuvers. These identify specific technological, doctrinal, and organizational changes that the Army must undertake. Begun in 1992, this grew into the "Force XXI" process that uses battle laboratories, warfighting experiments, and advanced technology demonstrations to generate and test ideas.[9] Force XXI seeks to harness information technology to create a "digitized force" that can dominate the battlefield by operating with greater speed and knowledge than opponents. Technology, in this vision, will compensate for occasional quantitative disadvantages and minimize U.S. military casualties.

In the mid-1990s, Army Chief of Staff General Dennis Reimer decided that his service needed to look even deeper into the future than Force XXI or *Army Vision 2010*. The pace of change in the modern world had become so intense, Reimer concluded, that the Army needed to extend its strategic planning horizons. Since the main weapon platforms of the Army, including the Abrams main battle tank, the Bradley fighting vehicle, and the Apache attack helicopter were expected to approach obsolescence around 2015, General Reimer thought it necessary to begin deciding whether the Army should seek a new generation of tanks, fighting vehicles, and helicopters, or point toward radically different systems because of technological and strategic change.

The framework for this long-term planning is the Army After Next Project, a series of wargames, workshops, studies, and conferences which explore feasible strategic environments of the 2020-2025 period and speculate on the sort of technology, force structure, and operational concepts that the Army might need. One of the most crucial parts of the Army After Next process has been identifying the most likely or dangerous type of enemy. *Speed and Knowledge*, the annual report of the project, singles out what is called a "major military competitor,"[10] a nation-state that threatens the United States or U.S. interests but cannot or does not emulate the digitized American military. Such an enemy might attempt to offset technological inferiority with relatively cheap counters such as land and sea mines, distributed air defense, coastal seacraft, submarines, inexpensive cruise and ballistic missiles, and unsophisticated weapons of mass destruction. Quantity would substitute for quality. The Army After Next Project seeks to design a force with superior operational and decisional speed, strategic mobility, and battlefield awareness to defeat such an enemy.

The Army After Next Project assumes that the proliferation of precision weapons will make the battlefield of 2025 so deadly that the defensive will be strengthened, making extended maneuver possible only when the enemy's advanced systems have been degraded and when one's own forces have high degrees of mobility and speed. Mobility and speed will allow distributed, decentralized operations at a very high tempo with what are described as "cascading" effects. "Tactical success," according to *Speed and Knowledge*, "piled up nearly simultaneously across the entire battlespace, could then lead under the right circumstances to operational-level disintegration as the enemy's plans are first foiled and then shattered—even as his ability to control his own forces evaporates before he can respond."[11]

The Army After Next will be built on knowledge accruing from advanced information technology, specifically “a largely space-based ‘living internet’ of a jointly-integrated, multilayered C^{4}ISR system of systems that permits the fusion of information products from a variety of sources, from national to tactical level” all leading to “a coherent, near real time, common picture of the battlespace.” The report states that “knowledge is paramount...the unprecedented level of battlespace awareness that is expected to be available will significantly reduce both fog and friction.” It continues:

> Knowledge will shape the battlespace and create conditions for success. It will permit…distributed, decentralized, noncontiguous operations….It will provide security and reduce risk. Through the identification of enemy strengths, weaknesses, and centers of gravity, coupled with near complete visibility of friendly force status and capabilities, knowledge will underwrite the most efficient application of all elements of military power—enabling higher tempos of operations. Knowledge will also focus and streamline the logistics support required to maintain high tempos.[12]

Organizationally, the Army After Next Project projects a hybrid U.S. Army combining advanced components with “legacy” forces. Specifically, the Army of 2025 is expected to have four parts: contingency forces including Battle Forces, Strike Forces, light and selected mechanized forces; Campaign Forces; Homeland Defense Forces; and Special Forces.[13] With such a combination, the future U.S. Army would retain a great deal of flexibility and be better able to operate in coalition with allies who had not built digitized forces. Throughout the project, though, emphasis remains on countering cross-border aggression against a state where the U.S. had economic interests by another state using combined arms warfare with a few additional technological twists and capabilities. Invariably, the "blue" forces emerge victorious.

The U.S. Air Force's vision of future war is also characterized by a combination of creativity and conservatism. *Air Force 2025*, commissioned by the Chief of Staff of the Air Force to examine the concepts, capabilities, and technologies that the United States will require to remain the dominant air and space force for the future, is a cauldron of new, creative thinking. It solidified the position of the Air University as the U.S. military's cutting edge source of ideas. Often using teams led by a colonel or lieutenant colonel rank and with a number of majors, *Air Force 2025* provided comprehensive examinations of topics such as information warfare, unmanned aerial combat platforms, organizations to deal with the gray area between peace and war, and assessing ways to most efficiently erode an enemy's unity and will.[14]

To some extent, official Air Force strategy statements are more radical than those of the Army. For instance, the *Air Force Strategic Plan* notes that exotic technologies such as micro-technology, biotechnology, and nanotechnology could alter the shape of future battlefields. It even admits that technological breakthroughs could potentially allow the rise of a global "peer competitor."[15] But generally, the Air Force's senior leaders see future warfare as an extrapolation of the 1990s with advanced technology added on. The *Air Force Strategic Plan* indicates that non-state enemies and asymmetric strategies will pose challenges as will new warfare environments like the infosphere, space, and urban areas, but assumes general continuity in strategy and the nature of conflict. Ironically, the Air Force planning document notes the ongoing diffusion of information technology and the commercialization of space, but does not suggest that these might challenge the notion of "information superiority" on which *Joint Vision 2010* is built.

The Sea Services also subscribe to the notion that future warfare will be a high tech version of late 20th century combat. But the Marines, at least, look seriously at fairly radical changes in tactical and operational procedures, including new organizations and doctrine. In fact, the Marines are in many ways the service most amenable to new concepts. The Marine Corps After Next (MCAN) Branch of the Marine Corps Warfighting Laboratory, for instance, is exploring what it calls a "biological systems inspiration" for future warfighting. According to its web site:

…for the last three centuries, we have approached war as a Newtonian system. That is, mechanical and ordered. In fact, it is probably not. The more likely model is a complex system that is open-ended, parallel, and very sensitive to initial conditions and continued "inputs." Those inputs are the "fortunes of war." If we assume that war will remain a complex and minimally predictable event, the structures and tactics we employ will enjoy greatest success if they have the following operational characteristics:

- dispersed,
- autonomous,
- adaptable,
- small.

The characteristics of an adaptable, complex system closely parallels biology. For that reason, much of the efforts of MCAN focus on exploiting biological inspiration in future military systems.[16]

By “biological systems inspirations” the Marines mean things like biomimetic engineered materials; small, “bug like” robotics; neural or neuronal nets capable of complex, adaptive responses; parallel computers; and, nanotechnology. In addition, the Marines have been at the forefront of efforts to understand and develop weapons with “tunable” effects, especially non-lethal weapons.[17]

The Navy, by contrast, is the service most resistant to change. Its view of future warfare offers few ideas that are not based on existing weapons platforms, particularly the carrier battlegroup and cruise missiles fired from surface platforms or multi-purpose submarines.[18] The Navy did briefly discuss a futuristic semi-submerged “arsenal ship” which could carry 500 cruise missiles and be manned by a crew of as few as 50, or even be unmanned,[19] but even then, Navy leaders were hesitant to consider this revolutionary. According to Admiral Jay Johnson, Chief of Naval Operations, “My view of Arsenal Ship is one that says Arsenal Ship IS NOT a replacement for an aircraft carrier. People who say it is do not understand the concept as we envision it. Arsenal Ship to me has great potential as a complementary capability to a battlegroup.”[20] Eventually, the Navy lost interest in the arsenal ship and the project petered out.[22] The Navy’s unwillingness to consider that high signature targets like aircraft carriers might some day be vulnerable is one illustration of the hubris endemic in the official vision of future warfare. Unassailable U.S.

technological superiority and "full spectrum dominance" are articles of faith.

Elsewhere within the Department of Defense, the search continues for ways to apply new technology to traditional force-on-force combat. The Defense Science Board, for instance, has speculated on a new land-based military unit which would be light, agile, and potent, operate in a distributed and desegregated fashion, utilize high situational awareness generated by information technology, depend on remote fire, be connected by a robust information infrastructure, and and be supported by precision logistics.[22] Such an organization could provide a rapid intervention capability and prepare a theater for heavier units that would arrive later. It would fight for 2 weeks or less and then be reinforced or withdrawn. The basic element would be "combat cells" which would make extensive use of unmanned vehicles and robotics, using humans "only when necessary." It would avoid direct firefights, remain dispersed most of the time for survivability, and mass only to repulse a major attack. Information technology would be central: "A key capability for combat cell mission success is maintaining a local awareness bubble larger than the enemy's."[23]

In their thinking about the future, all the services agree that the U.S. military needs a highly capable, rapidly deployable expeditionary unit. The core concept behind this is "strategic preclusion," which in a crisis would allow the U.S. to achieve demonstrable battlefield dominance before an enemy has completed "operational set."[24] This would force an opponent to either concede or face inevitable massive defeat.

Again, the expectation is that future warfare will be a reprise of *Desert Storm*—unambiguous, cross-border aggression by one state against another. The services offer few explanations of why U.S. political leaders would use military force early when the traditional approach is to use it as a last resort. Similarly, there is little indication of how future strike and expeditionary forces might be used against nontraditional or ambiguous aggression.

The official vision of future information warfare follows a similar logic. Despite immense debate over this topic within the intellectual communities of the services and the Department of Defense, the general notion is that information is an "enabler" of traditional forms of military activity. Information warfare is seen as "an amalgam of warfighting capabilities integrated into a CINC's theater campaign plan...."[25] The assumption is that technological prowess will allow U.S. forces to overcome threats to their information technology. *Joint Doctrine for Information Operations* defines information operations as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[26] While official thinking accepts the fact that information technology has had a "revolutionary" impact on life, this revolution is thought to have cemented the strategic realities of the past where the U.S. military was able to defeat enemies through technological advantages. In other words, the "Information Age" U.S. military will be much like the pre-information age U.S. military, only faster and smarter.

Overall, the official view of the future sees technology in general, particularly information technology, as an enabler or force multiplier, not as a locomotive for a revolutionary transformation of the security environment or the nature of warfare. Concepts such as “strategic preclusion,” “full spectrum dominance,” and “information superiority” reflect the situation of the 1990s—a qualitatively dominant U.S. military focused on deterring or defeating traditional cross-border aggression by one state against another. Most official documents accede that future enemies will attempt asymmetric methods, but it is what might be called a “moderate” asymmetry rather than a radical type. Official discussions of technologies that might have potential to be transformative—nonlethal weapons, information warfare technologies, robotics, and so forth—are conservative, seeing these things as support systems in conventional warfighting rather than new modes of warfare. With the exception of adding three new tasks for the U.S. military—space operations, information warfare, and homeland protection—the official vision anticipates no or few strategic shifts. In general, 21st century war will be in many ways like mid- or late-20th century war, with new technology allowing future generals and privates the ability to do well what past generals and privates could only dream of.

The Technological Alternative

The notion that future warfare will remain a state-on-state venture between conventionally organized armed forces with the United States holding a clear technological superiority is certainly not limited to official thinking. George and Meredith Friedman, for instance, argue that technology will give the 21st century U.S. military the capacity to hit targets with greater and greater precision, thus making the new century “an American century.”[27]

But there are visions of future warfare with a different perspective. One genre focuses on technology. This assumes that emerging technology will force or allow truly radical change in the conduct of armed conflict rather than simply augmenting current capabilities as the official vision anticipates. For instance, technological breakthroughs or sustained progress in several areas may allow effective autonomous systems—robots—to supersede humans in many warfighting functions.

Coming decades are likely to see the proliferation of robots around the world and in many walks of life. Hans Moravec, for instance, contends that mass produced robots will appear in the next decade and slowly evolved into general purpose machines.[28] As one of the most avid customers of new technology, this will certainly affect the U.S. military. Initially, the prime function of military robots might be in dangerous or tedious functions. Examples of the latter might include evacuation of casualties under fire; operating in environments where nuclear, biological, or chemical weapons have been used; mine clearing; fire fighting; and reconnaissance, surveillance, and target acquisition.[29] The real breakthrough and decision point will come when robots advance to the point that they have potential for combat use. This will take some time, particularly for land warfare. Using robots in “clean” operating environments like air, space, and sea will be easier than the ground, which poses severe challenges for autonomous systems in terms of movement, sensing, and decision-making. Robots intended for battlefield use will have to be orders of magnitude “smarter” than those used for less stressful functions such as loading and moving material.[30]

Current thinking about the technological characteristics of future military robots moves along two tracks, each synthesizing robotics and other emerging technologies. The first envisions autonomous systems employing sensors, computing, and propulsion different from that used by people. One of the goals in this arena is miniaturization. The Pentagon already has a $35 million program under way to develop a bird-like, flapping-wing micro-air vehicle for battlefield reconnaissance and target acquisition.[31]

This is just the beginning. The true revolution could come from the maturation of micro-electro-mechanical systems, or MEMS. MEMS technologies construct tiny mechanical devices coupled to electrical sensors and actuators.[32] MEMS could allow things like a “robotic tick” the size of a large insect to attach itself to an enemy system such as a tank, then gather and transmit information or perform sabotage at a designated time.[33] In a fanciful but feasible description of the future battlefield, James Adams writes:

MEMS opens a window on a new generation of technology that will literally transform the battlefield. Tomorrow’s soldier will go to war with tiny aircraft in his backpack that he will be able to fly ahead of him to smell, see, and hear what lies over the hill or inside the next building. Additional intelligence will be supplied by sensors disguised as blades of grass, pockets of sand, or even clouds of dust.[34]

However radical such a notion might seem, it is, like the official vision of the future, essentially new technology used in old ways. In contrast, futurists like

Martin Libicki have speculated on truly radical modes of warfare that make use of MEMS-based robotic technology. Libicki's alternative vision of future war is profound and creative. Its essence is that information technology, among other things, is shifting the advantage in warfare to "the small and the many" over "the large, the complex, and the few." This is in stark contrast to orthodox U.S. strategic thinking that seeks ever more capable systems that are more expensive and thus acquired in smaller numbers.

Based on the superiority of "the small and the many," Libicki describes three stages. He calls the first "popup warfare." This is based on extant technology in a security environment characterized by the proliferation of precision guided munitions (PGMs). While *Joint Vision 2010* and other official documents expect many states to have precision guided munitions, they assume that the U.S. military can overcome enemy PGMs by stealth, operational dispersion, and speed. Libicki is more skeptical. "The contest between stealth and anti-stealth will be long and drawn-out," he writes, "but…the betting has to be against stealth for any platform large enough to encompass a human...even with stealth, everything ultimately can be found."[35] The result will be "popup warfare" where both sides stay hidden most of the time, pop up just briefly to move or shoot, and then "scurry into the background."[36]

Libicki's second stage of future warfare, which he calls "the mesh," uses technologies available over the next 20 years against an enemy with developed industry but underdeveloped informational capabilities. To a large extent, this is coterminous with the official vision that calls for an inter-linked mesh of sensors and information technology to give American commanders a clear and perfect view of the battlefield while their opponents remain in the dark. Reinforcing the assumptions found in *Joint Vision 2010* and other official documents, Libicki writes, “Tomorrow’s meshes will allow their possessor to find anything worth hitting.”[37]

Libicki’s third stage represents the ultimate ascendance of “the small and the many.” He contends that eventually enemies will develop capabilities to the point that platforms like surveillance aircraft and satellites that compose the American military’s “mesh” will be vulnerable to attack. The solution is to weave a mesh composed of small, moderately priced objects rather than a handful of very large and very expensive ones. “Battlefield meshes, as such, can be built from millions of sensors, emitters, and sub-nodes dedicated to the task of collecting every interesting signature and assessing its value and location for targeting purposes.”[38] This is where MEMS-based robotics becomes significant. Libicki speculates on the value of ant-like robots, each with a fairly limited capability. But when weaved together, their collective capacities generate extensive capabilities. The inherent redundancy of the mesh in what Libicki calls “fire ant warfare” would make it much more robust than the one envisioning in official documents.

While the first track of thinking about robotics concentrates on miniaturization and the integration of networks of small robots with relatively limited functions, the second track deals with partially organic robots—“cyborgs” of one type or the other. Often the subject of science fiction, such things are not as technologically far-fetched as it might seem. For instance, since the objective in covert surveillance is not to avoid being seen, but to avoid being noticed, it might be possible to mount cameras or other sensors on dogs, rats, insects or birds if implants to steer them could be developed. Research scientists are already experimenting with placing very small mechanical components into cockroaches.[39]

Simple cyborgs like this may be only the beginning of an even more fundamental revolution, or more precisely, marriage of several ongoing technological revolutions. Lonnie D. Henley, for one, argues that a melding of developments in molecular biology, nanotechnology, and information technology will stoke a second generation revolution in military affairs.[40]

For example, nanotechnology is a manufacturing process that builds at the atomic level.[41] It is in very early stages, but holds the possibility of extremely small, perhaps microscopic, machines. Eric Drexler, the most fervent advocate of nanotechnology, predicts that it will unleash a transformation of society as self-replicating nanoborobots manufacture any material permitted by the laws of nature and thus help cure illness, eliminate poverty, and end pollution.[42] As Henley points out, combining nanotechnology with molecular biology and advances in information technology could lead to biological warfare weapons that are selective in targets and are triggered only by specific signals or circumstances. It could lead to decentralized sensor nets, perhaps millions of microscopic airborne sensors or a mesh of very small robots as envisioned by Libicki. And, Henley contends, it might eventually be possible to incorporate living neuron networks into silicon-based computers, greatly augmenting their "intelligence." In such a world, the *JV 2010* future, or even that of advanced programs like the Army After Next Project, will fade into obsolesce.

Beyond technological obstacles, the potential for effective battlefield robots raises a series of strategic, operational, and ethical issues, particularly when or if robots change from being lifters to killers. Developing the “rules of engagement” for robotic warfare is likely to be extraordinarily contentious. How much autonomy should robots have to engage targets? As a robot discovers a target and makes the “decision” to engage it, what should the role of humans be? How would the deployment of battlefield robots affect the ability of the U.S. military to operate in coalition with allies who do not have them, given that a roboticized forces is likely to take much lower human casualties than a non-roboticized one? Should the U.S. attempt to control the proliferation of military robotic technology? Is this feasible since the evolution of robotic technology, like information technology, will largely take place in the private sector? Should a fully roboticized force be the ultimate objective for the U.S.? Ultimately, the decision criteria used to answer these questions will be as much ethical as technological.

The Organizational Alternative

Other visions of the future focus on alternative means of organizing militaries and, by the same stroke, organizing warfare. To some extent, current official thinking recognizes this possibility, stressing the rise of asymmetric challenges to the U.S. military. In fact, asymmetry has become one of the central concepts in thinking about the future of warfare within the Department of Defense and the military services. While *Joint Vision 2010* does not explicitly mention asymmetry or asymmetric counters, all key planning documents now do. The Air Forces’ *Global*

Engagement notes that “hostile countries and non-state actors [will] seek asymmetric means to challenge US military superiority;” the *1998 Annual Report of the Army After Next Project* contends that “major competitors will probably develop creative asymmetric strategies;” and the *1999 Joint Strategic Review* provides an in-depth analysis of the implications of asymmetric methods.

The reason is simple: the Gulf War seemed to show that the United States cannot be defeated in symmetric conflict, particularly when the enemy relies on Soviet equipment and Soviet-style methods and U.S. national interests are clear. If anything, the gap between the U.S. military and opponents who might attempt force-on-force combat in open terrain is growing. No potential enemy will soon undergo an information-based revolution in military affairs. But enemies still feel the need to challenge the United States. As a result, they are or will seek asymmetric methods. The question then becomes, “What forms of asymmetry will be most common and most problematic for the United States?”

In Washington, study groups wrestle with this issue while core strategic documents struggle to define, assess, and bound asymmetry. So far, official thinking has focused on a few forms of asymmetry such as the use of precision guided munitions or weapons of mass destruction to deter or complicate power projection into a theater of war, the use of terrorism to erode public support for the employment of military forces, the use of quantity to compensate for qualitative disadvantages, and the use of complex terrain, particularly urban settings. Other thinkers offer more radical notions of asymmetric enemies, speculating on enemies who use radically asymmetric strategies and organizations rather than methods. The most important of these deals with the potential rise of enemies organized as networks rather than hierarchies.

One of the macro-level results of the Information Revolution has been a shift in effectiveness from centrally controlled or commanded hierarchical organizations to those composed of interlinked, networked nodes. This has certainly characterized the business world over the past few decades. Increasingly, it affects politics as well. As the late Carl Builder and Brian Nichiporuk wrote, "Since so many of the institutions of the nation-state are hierarchical and so many of the transnational organizations are networked, the net flow of power today tends to be out of the nation-state and into nonstate actors."[43] Soon, this same process will touch the militaries and warfare. As a result, future enemies likely to pose the most complex problems for the U.S. military are those organized as networks. This means non-state actors.

Some of the most creative thinking on networked enemies has been done done by John Arquilla and David Ronfeldt. They distinguish "cyberwar," in which state military forces fight each other using information-related principles and technology, from "netwar" in which non-state, paramilitary, and other irregular forces use coercive violent means short of traditional war.[44] The advent of netwar is part of a larger process that Martin van Creveld calls "irregularization" of warfare.[45] Arquilla and Ronfeldt contend that:

…the information revolution favors and strengthens network forms of organization, while making life difficult for hierarchical forms. This implies that conflicts will increasingly be fought by "networks" more than by "hierarchies." Thus, whoever masters the network form should gain major advantages in the new era.[46]

Networked enemies will be made up of dispersed and varied groups which coordinate their actions but often do so without centralized control or even explicitly common objectives. As Arquilla and Ronfeldt note, a variety of criminal and violent political organizations are evolving in this direction. Of course, enemies organized as networks are not new. The Viet Cong, the Somali militias, and the Colombian narco-traffickers were all networks to a greater or lesser extent. But the key change is that the Information Revolution is making networks infinitely more effective than in the past, primarily by opening avenues for broadband instantaneous communication and coordination. Groups that would never have been aware of each other's existence in the past, much less coordinated, can now visit each other's web sites and link through e-mail, newsgroups, internet relay chat, or other electronic means.

If Arquilla and Ronfeldt are correct, the most problematic enemy the United States will face in the future may be a network of opponents unified only by their opposition to Washington or to a U.S.-dominated world economic and political system. Nothing like this is evident today, but it is possible to speculate on what a networked enemy might look like. It would overlap state borders. Some components would exist primarily outside the U.S., and some within. The network would probably include a range of criminal organizations from traditional ones like narco-traffickers and arms smugglers to more modern ones specializing in computer crime. The latter would provide information warfare expertise and form one of the most dangerous nodes of the network. The network would also be likely to include a variety of political or ideological groups opposed to American policy, including ethnic separatists, anti-government militias inside the U.S., violent environmentalists, anti-change radicals, and those who subscribe to anti-authority ideologies which emerging in the computer hacker community.

In all likelihood, only portions of the network would be violent. Non-violent, legal components would explicitly or implicitly work in concert with other, more violent nodes. The non-violent, legal components would, among other things, lead campaigns to weaken the U.S. military by having certain technologies or methods banned or proscribed. This tendency is evident today: As the U.S. seeks to develop effective nonlethal weapons, a global anti-nonlethal weapon movement is coalescing. The same may happen for other new technologies which give the U.S. military an advantage including space-based weapons, some types of information warfare technology, directed energy weapons, the military applications of nanotechnology and biotechnology, and military robotics.

On the offensive, a networked enemy would “swarm.” Rather than explicitly coordinating a strategy, they would organize their own strikes—whether using traditional violence, cyberviolence, or psychological and political means—to have a symbiotic effect. Because networked forces can “maneuver well within the decision making cycle of more hierarchical opponents,” they can “reinforce the original assault, swelling it; or they can bunch swarm attacks upon other targets, presenting the defense with dilemmas about how to best deploy their own available forces.”[47]

Networked enemies tend to be redundant and diverse, meaning that anyone attacking them must have a very wide range of capabilities. They will not have a "center of gravity" in the traditional sense, thus making traditional military methods of strategic and operational planning irrelevant.

Networked enemies will make great use of ambiguity, often operating at the boundaries between military and law enforcement functions, national and international jurisdictions, legal and illegal activities, and war and peace. Traditionally, the United States has serious problems with any form of conflict that makes use of such ambiguities. Among other problems, ambiguity tends to cloud the U.S. decision-making process and thus constrain the military. At the same time, the ability of a networked enemy to adapt rapidly—to replicate success and find solutions to failures—will make it difficult for a hierarchy like the U.S. military keep up with them. Arquilla and Ronfeldt contend that to match networked opponents, governments much develop network/hierarchy hybrids like those taking shape in the corporate world.[48] Advanced official visions of future warfare such as the Army After Next Project, the Marine Corps After Next and Sea Dragon programs, the Air Force's *New World Vistas*, the Defense Science Boards 1996 Summer Study, and the Navy's *Forward…From the Sea* envision land warfare networked at the tactical level, with dispersed swarming combat cells as key units.[49] But no official vision seriously considers the challenges of fighting networked enemies. This may contribute to their rise.

The U.S. military envisioned in *JV 2010* or even the Army After Next Project, designed as they are for "near peer competitors," "regional competitors," and the like, would be inadequate against such a networked enemy. American strategists would probably focus on other states which supported or were part of the network, but deterring or defeating these states would not necessarily lead to the downfall or collapse of the network. Information technology is, then, a double edged sword. It provides the U.S. military with the chance to attain dominant battlespace awareness against conventional state enemies, but it also opens the way for the emergence of dangerous and complex unconventional enemies.

The Environmental Alternative

Since the 1930s, one of the enduring debates among military thinkers has concerned the feasibility of truly strategic warfare. Some like the American Billy Mitchell and the Italian Guilio Douhet argued that technology, specifically the technology of aircraft, provided the opportunity to bypass military forces in the field and defeat an enemy by striking directly at his homeland.[50] This, they felt, represented a profound change in military strategy.

History did not bear them out. Strategic bombing campaigns contributed to Allied victory in the European and Pacific theaters during World War II, but only in conjunction with more traditional land and sea operations. Strategic bombing not accompanied by invasion such as the German blitz against England and, later, the American bombing of North Vietnam failed to bring decisive results.

Today, the debate has reemerged between what Michael L. Brown calls the “strategic attack paradigm” and the “operational attack paradigm.”[51] The more conservative approach within the strategic attack school comes from advocates of airpower. Thinkers like John Warden hold that vast improvements in technology mated with a more sophisticated understanding of what holds a state together and what can cause one to collapse make the vision of people like Douhet attainable.[52] More radical perspectives assume that information technology has opened a whole new environment for the conduct of warfare. Specifically, a handful of strategists predict the emergence of strategic information warfare: Decisively coercing an enemy by information technology attacks on his information infrastructure.

The idea that information technology is driving a profound transformation in all aspects of human life, from the political and economic to the cultural and normative, is widespread. Michael Vlahos, for instance, argues that human life is shifting to what he calls the “infosphere,” which is “the fusion of all the world’s communications networks, databases and sources of information into a vast, intertwined and heterogeneous tapestry of electronic interchange.”[53] Analysts like Robert Bunker think that this will lead to a fundamental change in the nature of warfare, not simply the appliqué of microprocessor based technology as in the official vision of the future, but the addition of a fifth dimension of warfare to three-dimensional space and time.[54] In stark contrast to the official vision of the future, Bunker holds that the United States is unlikely to attain dominant battlespace knowledge in cyberspace, whether in what he calls the upper tier (the Internet and the electromagnetic spectrum) or the lower tier (stealth masking of physical forces).

But, he admits other state militaries will do no better, so the prime enemy will be non-state actors, often criminals, with the flexibility and creativity to make use of cyberspace's potential. For the U.S. military to be truly successful, Bunker argues, it must master new concepts like cyber-shielding, cyber-maneuver, and what he calls "bond-relationship" targeting that creates "tailored disruption within a thing, between it and other things, or between it and its environment by degrading, severing, or altering the bonds and relationships which define its existence."[54]

Conceptually, strategic information warfare is the descendent of strategic bombing since its prophets assume that a nation can suffer defeat while its military forces in the field remain intact. The logic behind strategic information warfare, as Alvin and Heidi Toffler explained, is that information has become the major source of wealth for advanced states.[55] Almost all aspects of modern economies depend on information technology. Most wealth itself is held in electronic rather than physical form today—95 percent of American wealth, for instance, is digitally represented.[56] Because national information assets and information infrastructure are the source of economic strength, attacking them could bring a nation to its knees. As RAND Corporation study notes, strategic information warfare is characterized by low entry cost; blurred traditional boundaries between public and private interests, law enforcement and national security, etc.; an expanded role for perception management; a new strategic intelligence challenge; formidable tactical warning and attack assessment problems; difficulty building and sustaining coalitions; and vulnerability of the U.S. homeland.[57]

The official Department of Defense vision of future warfare incorporates what is often called "first generation" strategic information warfare, in which information attack and defense is one component of military strength such as conventional forces and weapons of mass destruction.[58] Second generation strategic information warfare would be a "stand alone" capability in which information attacks themselves bring decisive or strategically significant results. If second generation strategic warfare becomes a serious security threat, much of what is accepted practice within military strategy will be eroded or obviated. In all likelihood, other states will not be the main users of strategic information warfare. Not only are other states wedded to traditional notions of military force, but it will be possible in most cases for the U.S. to deter them by other means—"if you attack our information infrastructure, we will bomb your bridges, etc."

Non-state enemies, though, may have the means and the incentive to use strategic information warfare. Because they have no home territory and are less bound by the laws and ethics of international behavior, they will be more difficult to identify and deter.[59] They will, in many cases, be more flexible and adaptable than U.S. security forces, shifting methods and strategies much more quickly than states. They will be able to hire the best available talent with fewer political, ethical, and legal constraints than states. They will be able to play on divisions and boundaries within states, whether geographic or organizational ones. Strategic information warfare will be extraordinarily difficult for state security services because of its ambiguity. Knowing when one is under attack will be difficult, but identifying the attackers even more problematic.

Many of the elements of traditional military strategy—centers of gravity, mobilization, phased operations, deployment, decisive victory, military professionalism, civil-military relations—will have no meaning or radically different meanings in the face of strategic information warfare. It is far from clear what role the U.S. military might play in defending against it. And, as with any type of security threat, there is the danger that fear of strategic information warfare will lead the U.S. to take steps to defend itself that themselves become debilitating. Just as a society can become militarized and ossify in the traditional sense when facing a sustained threat, a society obsessed with defense against strategic information warfare can defend itself to the point that its electronic commerce and other aspects of the economy are hindered.[60]

Conclusions

Information technology has many effects in the modern world. To one extent, it is a leveler, making comparative advantage of short-lived. Others learn of advantages, develop an understanding of them, and replicate or improve them quickly. Greek fire—a military technology the Byzantines kept secret for centuries—cannot be replicated. Businesses around the world learned this lesson well. Successful ones instigated programs to defend their intellectual advantages as much as possible. More importantly, they have undertaken deep changes in organization and organizational culture to stoke the pace of innovation and change, moving to the next innovation as quickly as others adopt past innovations.

Armed forces, even the U.S. military, which is the most adaptive and advanced in history, will struggle to replicate this in coming decades. They will face networked enemies with the capacity for rapid change, reaction, and adaptation. They will be forced to fight in the infosphere in addition to (or perhaps in lieu of) traditional battlefields. Ironically, current U.S. national security strategy may provoke the emergence of creative, networked enemies using radically asymmetric methods precisely because it uses military force to create a form of stability that many outside the U.S. see as cultural and economic imperialism. The future U.S. military is likely to be the victim of the success and prowess of today's U.S. military. Because the current U.S. military gives every indication of retaining its superiority at traditional types of combat, smart enemies will eschew them. Creativity will emerge from frustration and desperation.

Information technology is a classic dual-edged sword. It is the greatest source of empowerment in human history, but like all new sources of power, it brings a degree of dependence which can create weaknesses. Current thinking about future warfare holds that victory will come to those with dominant battlefield awareness and information dominance. All bets are placed on a single card. Yet the nature of the infosphere and the world of information technology suggests that information dominance of the sort envisioned in *JV 2010* and other official documents may be infeasible. The technology for hiding signatures, whether through physical or electronic means, may advance as rapidly as the technology for sensing signatures.

In an even broader sense, the assumption of continued, perhaps eternal, American technological supremacy is hubris. Information technology disperses knowledge. In the past, a fairly firm distinction existed between military technology and non-military technology. Because the United States spent more than any other nation on military research and development, it retained a technological edge. But in the Information Age, the distinction between military and non-military technology is blurred. Because most research and development in information technology takes place in the private sector where it is available to anyone with money, the chances of the U.S. retaining the sort of technological advantage over any conceivable enemy that it did in the past may be fading. The United States may not face a state military in the future that is technologically superior, but the chances are good that it will face some sort of enemy that is technologically superior in some key arenas. When this happens, the most fundamental assumption of American military strategy no longer holds.

History suggest that a military only undertakes truly revolutionary change in the face of defeat or the perception of imminent defeat or danger. As Kenneth Allard points out, “Few more powerful inhibitors to military progress exist than victories, especially overwhelming victories against a lesser opponent.”[61] Eventually, Saddam Hussein may be responsible for the defeat of the U.S. military. He will never win on the battlefield, but he may have ossified the creativity of the American military by reinforcing the notion that prowess at digitized blitzkrieg is all that matters.

The ultimate question becomes whether the U.S. military can identify and adjust to the seminal changes that information technology is forcing or allowing without a major fiasco. It took disaster—the battles of

Jena and Auerstadt—for the Prussian military to undertake the changes that contributed to the eventual defeat of Napoleon and paved the way for 20th century industrial war managed by general staffs. Likewise, Germany's defeat in 1918 was the catalyst for blitzkrieg. No one knows whether the United States, without a Jena or Pearl Harbor, can adapt to enemies who fight differently than Saddam Hussein. The danger remains that the U.S. military will become like an armored knight of the late 16th century, the paragon of technological and doctrinal development in a type of warfare that had become obsolete. It remains to be seen whether the U.S. will recognize that its prowess and success have bred obsolescence before a major defeat or only afterwards.

A skeptical response to this may be easiest, but is not automatically correct. There is cause for hope. Perhaps there are deep veins of creativity within the U.S. military waiting to be mined. Perhaps the explosion of thinking about the long-term future may lead the U.S. military out of its obsession with old-style war and institutionalize respect for rapid adaptation and creativity. Perhaps the U.S. military will begin to consider the danger from enemies other than "near peer competitors" and the like. Perhaps basic principles—which can be prisons as well as strengths—will be re-examined as the Information Revolution moves on unabated. Perhaps the revolution unleashed by information technology will cause American leaders to question having a military profession separate from other professions, and instead have lateral movement at all points in a career in and out of the military, thus allowing more creative thinking and diminishing the problems of groupthink. Perhaps they will abandon the whole concept of doctrine, which slows the pace of adaptation. And, since, has Hans Moravec points out, one of the things that makes humans such an adaptable species is their extended childhood, perhaps the U.S. military will reverse the pattern by which younger service members are specialized in their duties while more senior ones become more general. Many ideas warrant consideration.

The existing futures-oriented programs within the U.S. military have value. Most studies, simulations, exercises and wargames undertaken today are probably wrong about the ultimate impact that information technology will have on the conduct of warfare and on military strategy. Nevertheless, by inculcating the need to think about the future, to think holistically, and to innovate, these efforts may help the U.S. military react and adapt with adequate speed once the true essence of future warfare becomes clear.

The potential for rapid adaptation exists within the U.S. military. The next step is to find a way to realize it.

[1] Hans Moravec, *Robot: Mere Machine to Transcendent Mind*, (New York,NY: Oxford University Press, 1999), p. 1.

[2] See the description in Ryan Henry and C. Edward Peartree, "Military Theory and Information Warfare," in Ryan Henry and C. Edward Peartree, eds., *The Information Revolution and International Security*, (Washington, DC: Center for Strategic and International Studies, 1998).

[3] *Joint Vision 2010*, (Washington, DC: Chairman of the Joint Chiefs of Staff, n.d.), pp. 14-15.

[4] *Ibid.*, p. 11.

[5] *Ibid.*, p. 24.

[6] Briefing by Admiral Harold W. Gehman Jr., Commander in Chief (CINC) of USACOM to the Joint Experimentation Futures Workshop, Breezy Point Naval Air Station, November 3, 1998.

[7] *Army Vision 2010*, (Washington, DC: Headquarters, Department of the Army, 1996), p. 2.

[8] *Ibid.*, p. 3.

[9] See *Force XXI...America's Army of the 21st Century*, (Washington, DC: Department of the Army, 1995).

[10] *Speed and Knowledge: the Annual Report on the Army After Next Project to the Chief of Staff of the Army* (July, 1997), p. 9-10.

[11] *Ibid*., p. 9.

[12] *Ibid*.

[13] *Second Annual Report of the Army After Next Project*, (Fort Monroe, VA: Headquarters, United States Army Training and Doctrine Command, December 7, 1998), pp. 11-13.

[14] See, for instance, Joseph A. Engelbrecht Jr., et al., "Alternative Futures for 2025: Security Planning to Avoid Surprise," a research paper presented to Air Force 2025, April 1996; William B. Osborne, et al., "Information Operations: A New War-Fighting Capability," a research paper presented to Air Force 2025, August 1996; Jeffrey E. Theiret, et al., "Hit 'em Where It Hurts: Strategic Attack in 2025," a research paper presented to Air Force 2025, August 1996; Bruce W. Carmichael, et al., "Strikestar 2025," a research paper presented to Air Force 2025, August 1996; and Edward F. Murphy, "Information Operations: Wisdom Warfare For 2025," a research paper presented to Air Force 2025, August 1996. These papers are available at http://www.au.af.mil/au/2025/

[15] *Air Force Strategic Plan*, pp. 11-12.

[16] http://208.198.29.7/mcwl-hot/home/index.html

[17] On the debate concerning nonlethality, see Douglas C. Lovelace, Jr. and Steven Metz, "Nonlethality and American Landpower: Strategic Context and Operational Concepts," (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 1998).

[18] See *Forward…From the Sea: The Navy Operational Concept*, (Washington, DC: Department of the Navy, 1997); and *Department of the Navy 1999 Posture Statement: America's 21st Century Force*.

[19] James Adams, *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere*, (New York: Simon & Schuster, 1998), pp. 125-126. See also Scott Gourley, "Arsenal Ship," *Popular Mechanics*, June 1996, reprinted at http://popularmechanics.com/popmech/sci/9606STMIM.html; "Arsenal Ship" page on the Federation of American Scientists Military Analysis web page, http://www.fas.org/man/dod-101/sys/ship/arsenal_ship.htm; Arsenal ship page on the Defense Advanced Research Projects Agency page, http://www.darpa.mil/tto/arsenal.html; and John Mintz, "Navy Developing Revolutionary Radio-Controlled Ships," *Seattle Times*, June 23, 1996, reprinted at http://www.seattletimes.com/extra/browse/html/altnavy_062396.html

[20] Interview with media at Naval Air Station Oceana on Aug. 9, 1996, reprinted at http://www.chinfo.navy.mil/navpalib/ people/ flags/johnson_j/cnoquote.html

[21] Katherine McIntire Peters, "Rough Seas for Navy Programs," GovExec.com, August 1998, http://www.govexec.com/ procure/ articles/98top/08a98s7.htm

[22] *Defense Science Board 1996 Summer Study Task Force on Tactics and Technology for 21st Century Military Superiority, Volume I: Final Report*, (Washington, DC: Office of the Secretary of Defense, 1996).

[23] *Ibid*., p. II-10.

[24] *Second Annual Report of the Army After Next Project*, pp. 5-6.

[25] *Information Warfare: A Strategy for Peace…The Decisive Edge in War*, (Washington, DC: The Joint Staff, n.d.), p. 2.

[26] Joint Pub 3-13, *Joint Doctrine for Information Operations*, October 9, 1998, p. II-10.

[27] George and Meredith Friedman, *The Future of War: Power, Technology, and American World Dominance in the 21st Century*, (New York, NY: Crown, 1996).

[28] Moravec, *Robot*, p. 25.

[29] Report from "Robotics Workshop 2020," sponsored by the U.S. Army Research Laboratory, Pasadena, CA, February 25-27, 1997, (McLean, VA: The Strategic Assessment Center of Science Applications International Corporation, June 1997), pp. B-2 to B-3.

[30] *STAR 21: Strategic Technologies for the Army of the Twenty-First Century, Technology Forecast Assessments*, (Washington, DC: National Academy Press, 1993), p. 148.

[31] Lee Gomes, "It's a Bird! It's a Spy Plane!—Pentagon Funds Research Into Robin-Sized Robots," *Wall Street Journal*, April 6, 1999, p. B1.

[32] H. Lee Buchanan, Deputy Director, Defense Advanced Research Projects Agency, testimony before the Subcommittee on Military Research and Development, Committee on National Security, United States House of Representatives, February 27, 1997.

[33] Report from "Robotics Workshop 2020," p. B-26.

[34] Adams, *The Next World War*, p. 125.

[35] Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, (Washington, DC: National Defense University Press, 1994), p. 23.

[36] *Ibid*., p. 21.

[37] *Ibid*., p. 24.

[38] *Ibid*., p. 29.

[39] Report from "Robotics Workshop 2020," p. A-8.

[40] Lonnie D. Henley, "The RMA After Next: Biology, Nanotechnology, Information Systems, and the Future of Warfare," unpublished manuscript.

[41] See Eric Drexler and Chris Peterson, *Unbounding the Future: The Nanotechnology Revolution*, (New York: William Morrow, 1991), reprinted full text at http://www.foresight.org/UTF/Unbound_LBW/index.html

See also the nanotechnology web page of the Foresight Institute at http://www.foresight.org/NanoRev/index.html

[42] David Voss, "Moses of the Nanoworld," *Technology Review*, (March/April 1999), pp. 60-62.

[43] Carl H. Builder and Brian Nichiporuk, *Information Technologies and the Future of Land Warfare*, (Santa Monica, CA: RAND Corporation, 1995), p. 35.

[44] John Arquilla and David Ronfeldt, "The Advent of Netwar," in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND Corporation, 1997), pp. 275-291.

[45] Martin van Creveld, *The Transformation of War*, (New York, NY: The Free Press, 1991).

[46] Arquilla and Ronfeldt, "The Advent of Netwar," p. 276.

[47] *Ibid*., p. 282.

[48] John Arquilla and David Ronfeldt, "Looking Ahead: Preparing For Information-Age Conflict," in Arquilla and Ronfeldt, eds., *In Athena's Camp*, pp. 461-2.

[49] Ryan Henry and C. Edward Peartree, "Military Theory and Information Warfare," in Ryan Henry and C. Edward Peartree, eds., *The Information Revolution and International Security*, (Washington, DC: Center for Strategic and International Studies, 1998), p. 117.

[50] See David MacIsaac, "Voices from the Central Blue: The Air Power Theorists," in Peter Paret, ed., *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, (Princeton, NJ: Princeton University Press, 1986).

[51] Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," in Alan Campen, Douglas H. Dearth, and R. Thomas Goodden, eds., *Cyberwar: Security, Strategy, and Conflict in the Information Age*, (Fairfax, VA: AFCEA International Press, 1996), pp. 39-43.

[52] John A. Warden III, "Air Theory for the Twenty-First Century," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues*, (Maxwell Air Force Base, AL: Air University Press, 1995). See also Jeffrey R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010*, (Maxwell Air Force Base, AL: Air University Press, 1996); and Thieret, et al., "Hit 'em Where It Hurts."

[53] Michael Vlahos, “Entering the Infosphere,” *Journal of International Affairs*, (Spring 1998), p. 498. See also Michael Vlahos, “The War After Byte City,” in Stuart J.D. Schwartzstein, ed., *The Information Revolution and National Security: Dimensions and Directions*, (Washington, DC: Center for Strategic and International Studies, 1996).

[54] Robert J. Bunker, “Higher Dimensional Warfighting: Bond-Relationship Targeting and Cybershielding,” a paper presented at “The Future of War,” the Ivan Bloch Commemorative Conference, St. Petersburg, Russia, February 24-27, 1999.

[55] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, (Boston: Little, Brown, 1993).

[56] Henry and Peartree, “Military Theory and Information Warfare,” pp. 116.

[57] Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, “Strategic Information Warfare: A New Face of War,” *Parameters*, (Autumn 1996), pp. 81-92.

[58] Roger C. Molander, Peter A. Wilson, David A. Mussington, and Richard F. Mesic, *Strategic Information Warfare Rising*, (Santa Monica, CA: RAND Corporation, 1998), p. 6. See also Sam Nitzberg, “The Cyber Battlefield—Is This the Setting for the Ultimate World War?” *Proceedings of the 1997 International Symposium on Technology and Society*.

[59] There is some debate on this point. Timothy Thomas feels that deterrence is possible. Others such as Richard Harknett are more skeptical. See Timothy L. Thomas, “Deterring Information Warfare: A New Strategic Challenge,” *Parameters*, (Winter 1996-97), pp. 81-91; and Richard J. Harknett, “Information Warfare and Deterrence,” *Parameters*, (Autumn 1996), pp. 93-107.

[60] Martin C. Libicki, *Defending Cyberspace and Other Metaphors*, (Washington, DC: National Defense University, 1997), p. 38-39.

[61] C. Kenneth Allard, “Information Warfare: The Burden of History and Hubris,” in Schwartzstein, ed., *The Information Revolution and National Security*, pp. 237-8.

PART TWO

INTRODUCTION

Officially, all branches of the U.S. military have embraced the so-called "Revolution in Military Affairs" (RMA). Driven by a belief in the capabilities and promises of Information Age technologies, all branches of the U.S. Armed Forces concur that the RMA promises to transform the way wars are fought.

Nevertheless, as the excerpts from official documents contained in the seven articles in this section illustrate, agreement about the existence of an RMA does not signify agreement about what the RMA means for warfare. The first article, the Joint Chiefs of Staff's *Joint Vision 2010*, provides a conceptual overview of four new operational concepts that, it is argued, are key to Information Age warfare: dominant maneuver, precision engagement, full dimensional protection, and focused logistics. *Joint Vision 2010* claims that U.S. capabilities in these four areas, made possible by advanced information and communication technologies, will lead to U.S. dominance across the full spectrum of possible conflicts. This full spectrum dominance, it is argued, will enable the U.S. to protect its national interests well into the 21st century.

Accelerating rates of change will nevertheless make the global future "more unpredictable and less stable," the Joint Chiefs argue. This, combined with a smaller force structure, will increasingly require joint operations between U.S. armed forces even as the possibility of surprise actions by real and potential enemies increases. At the same time, *Joint Vision 2010* recognizes that advancing technology will have an immense impact on military capabilities, strategies, tactics, and operations. Many of these technological advances are centered on information and communication technologies.

This, the Joint Chiefs stress, leads to the emerging importance of "information superiority." To *Joint Vision 2010*, information superiority means both that the fog and friction of war will be reduced, and that offensive and defensive information warfare capabilities must be developed. This will require the creation of enhanced operational concepts—dominant maneuver, precision engagement, full dimensional protection, and focused logistics—that together will yield full spectrum dominance, that is, as discussed earlier, the ability of U.S. forces to dominate warfare across the entire spectrum of possible conflicts.

But even in the Information Age, *Joint Vision 2010* recognizes, not everything will depend on technology. High quality people, innovative leadership, agile organizations, and enhanced material will also remain critically important. So too will affordability. *Joint Vision 2010* then leaves it to each service to flesh out details of how operational concepts and strategic insights will be implemented.

The next five articles in this section provide excerpts from each service's analysis (one each from the Army, Air Force, and Marines, with two, as will be explained later, from the Navy) of how military operations and warfare will change in the future, and about what each service must in turn do if it is to meet its responsibilities successfully, given advances made possible by the RMA. The excerpts concentrate on the impacts of Information Age technologies within each service's separate domain. As will be seen, each service has devoted considerable thought to developing visions both of the future of warfare in the Information Age and of the impact of Information Age technologies on its own operations. Notably, the separate service visions contain significant areas of agreement and potential for cooperation. Equally notably, significant areas of disagreement and competition exist between and among the visions as well.

In *Army Vision 2010*, the U.S. Army details its views of why the Army will remain important in the Information Age. It identifies five reasons: to fight and win wars, to provide military options other than war, to deter aggression, to foster enduring values, and to bond the nation to military objectives.

Army Vision 2010 then presents the Army's interpretation of what military operations and warfare will require in the Information Age. Stressing that the realities of post-Cold War international affairs showed that the theory of a "stand-off" approach to warfare was invalid, *Army Vision 2010* argues that the Army is a versatile force whose importance will continue to rise in the Information Age because of its utility across the entire spectrum of conflict: defending or liberating territory, punitive intrusion, conflict containment, leverage, reassurance, core security, and humanitarian operations.

Army Vision 2010 next turns to the way the Army intends to achieve full spectrum dominance. It identifies six “patterns of operations”—Project the Force, Protect the Force, Shape the Battlespace, Decisive Operations, Sustain the Force, and Gain Information Dominance—that it argues, in the first five instances align precisely with *Joint Vision 2010*’s four operational concepts of Dominant Maneuver, Precision Engagement, Focused Logistics, and Full Dimensional Protection. The sixth Army pattern of operation, Gaining Information Dominance, is “fundamental to each of the other five Army patterns of operation as well as each of the operational concepts in *Joint Vision 2010*.”

The Army, then, has clearly bought on to the importance of information dominance in future military operations and warfare. Most of the rest of *Army Vision 2010* detail how Army concepts track with Joint Chief concepts, providing tracking elements not only at the conceptual level but also at the enabler and specific technology level. Notably, in its discussion of information superiority and information operations, *Army 2010* stresses not only “offensive and defensive efforts to create a disparity between what we know about our battlespace and operations within it and what the enemy knows about his battlespace,” but also the role of PSYOPS and deception campaigns. This is a focus that appears but rarely in the commentaries of other services.

Understandably, and not surprisingly, the U.S. Air Force presents a different although not necessarily contradictory view of the future of conflict and warfare in its *Global Engagement: A Vision for the 21st Century Air Force*. Beginning its analysis from the perspective that U.S. military strategy must be focused on “an increasingly U.S.-based contingency force” and emphasizing that in the twenty first century “it will be possible to find, fix or track, and target anything that moves on the surface of the earth,” *Global Engagement* emphasizes the need to combine new technologies and new tactics with core values and high quality people.

Global Engagement stresses that the Air Force is already transitioning from an air force into an air and space force, with the end goal of becoming a space and air force. Information Age technologies are what is allowing—indeed, forcing—this transition, the Air Force maintains, as more and more key military functions such as intelligence, surveillance, and reconnaissance; warning; position location; weapons guidance; communications; and environmental monitoring migrate to space.

Identifying the Air Force’s core competencies as rapid global mobility, precision engagement, global attack, air and space superiority, information superiority, and agile combat support, *Global Engagement* provides a general overview in each area of how the Air Force will leverage new technologies and new tactics to enhance capabilities. It also notes that “information operations, and information warfare in particular, will grow in importance during the 21st century.” Emphasizing the continuing importance of core values and high quality people highly trained for the new requirements of twenty first century military operations, *Global Engagement* concludes with a discussion of how the Air Force plans to improve its efficiency and its business practices as the Air Force maintains its sense of community and enhances its ability to promote American objectives.

The fourth article in this section, the U.S. Navy's *Forward…From the Sea* takes a somewhat different approach than either the Army's *Army Vision 2010* or the Air Force's *Global Engagement*. Whereas both of the other services' vision statements emphasize either explicitly or implicitly the role of advanced information and communication technologies throughout their presentations, the Navy does not begin to address innovative measures of naval warfare based on Information Age technologies until the concluding pages of *Forward…From the Sea*.

Indeed, throughout most of its discussions, *Forward…From the Sea* stresses the Navy's ability to maintain highly ready forward-deployed forces without infringing on the sovereignty of other states. Basing its analysis on the Navy's contribution to the three main components of the United States. National Military Strategy, that is, peacetime engagement, deterrence and conflict prevention, and fight and win, *Forward…From the Sea* until its concluding pages is surprisingly traditional in comparison to the Army's and Air Force's joint vision statements.

In its concluding pages, though, it makes up for lost time. The Navy's innovation efforts, *Forward…From the Sea* reports, will examine operational concepts and doctrine, how the Navy organizes and commands its forces, the capabilities of future systems and platforms, the manner in which the Navy provides maintenance and supply support, and the way in which the Navy educates and trains its people. Many of these undertakings will clearly rely on Information Age technologies as the Navy intends to provide "information warfare capabilities for joint forces," to have forces that will be "integrated into networked command and control systems that provide a common tactical picture of the battlespace," and to link "the sensors and weapons systems of an entire force into a highly integrated network." Further, *Forward…From the Sea* stresses that "emerging precision and information capabilities rapidly are making traditional views—that specific platforms...and specific types of ordnance…have specialized roles—obsolete."

Despite this, as an action and vision statement, *Forward...From the Sea* presents a less than comprehensive picture of Navy undertakings, plans, and actions in regard to the Revolution in Military Affairs. Thus, this third volume of the *Information Age Anthology* offers a second and more comprehensive Navy document, the U.S. Navy's *Information Warfare Strategic Plan*.

In its *Information Warfare Strategic Plan*, the U.S. Navy first lays out its view of information operations. Defining information operations much more narrowly than its sister services, the Navy's definition concentrates on the hardware, software, and personnel involved with information based processes and information systems rather than on how these factors may be utilized to achieve policy goals.

The strategic plan then turns to the challenges of information warfare. Stressing that all services must develop highly-capable offensive and defensive IW capabilities if the U.S. is to achieve full spectrum dominance in conflict, the Navy's *Information Warfare Strategic Plan* recognizes that a significant challenge exists in "establishing IW applications for future integration in national policy." The Navy also maintains that the unfamiliar nature of IW, difficulties in identifying attacks on computer networks, and existing laws constrain the Department of Defense from becoming proactive in either defensive or offensive IW.

The Navy's *Information Warfare Strategic Plan* next provides an overview of Navy's assessment of the IW threat, observing that "with the advent of IW, the geographic sanctuary traditionally enjoyed by the U.S. is all but gone." The strategic plan lists several principles for the evolution of Navy IW. These include but are not limited to the principles that the Navy will conduct IW both as an integral part of joint operations and on a stand-alone basis; will apply a system design philosophy of modifying installed shipboard and aircraft systems for offensive and defensive IW whenever possible; will embed IW equipment and expertise in its force structure; will establish IW as a formal naval warfare mission area; and will apply a risk management philosophy to its defensive IW investments and efforts.

After detailing the evolution of Navy IW organizations, the strategic plan provides a "roadmap" of the Navy's defensive IW program. Specific steps include but are not limited to identifying critical information systems; establishing the means to model vulnerability of systems, consequences of different types of attack on those systems, and means of post-attack restoration; apply the information gained in these models to design new systems; improve information attack identification capabilities; develop the ability to respond to and defend against such attacks; establish a Red Team to simulate attacks; establish counter-intelligence capabilities to cope with IW threats; and establish a close liaison with civilian and other government agencies that are developing defensive IW strategies and tactics.

The strategic plan concludes by addressing specific Navy courses of action in each of seven “Strategic Action Areas”: policy and doctrine, organization, career development, training and education, research and development, acquisition, mission planning and simulation, and intelligence support. Each of these seven areas is divided into three sub-sections, background, desired outcome, and course of action. Together, the courses of action detailed in these seven areas provide a comprehensive understanding of where and how the Navy intends to proceed in developing its information warfare capabilities.

The U.S. Marines discussion of the RMA and joint operations contained in *Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore* for the most part takes an approach closer to those of the Army and the Air Force than that of the Navy. Although *Operational Maneuver from the Sea* (hereafter *OMFTS*) does not provide the wealth of detail about information technologies and their impacts on operations found in *Army Vision 2010* or *Global Engagement*, *OMFTS* from its very introduction discusses a new series of threats and enhanced capabilities that are either based on or enhanced by Information Age technologies.

OMFTS presents a startlingly realistic picture of the evolving global strategic situation. Pointing to the breakdown of global order, the growing importance of non-state actors, the rise of regional powers, and the possible rise of another superpower as security challenges that the U.S. either faces or will face, *OMFTS* notes that “new weapons” will “inevitably be wielded by at least some of our enemies.” These may include at one extreme weapons of mass destruction, at the other extreme new ways of “blowing up dams and poisoning water supplies,” and in between “military applications of new technologies” that will have a “profound impact on where we fight, who we fight, and how we fight.”

How, then, should the United States, and more specifically the U.S. Marines, respond to this world of “chaos in the littorals,” as *OMFTS* terms it?

First, *OMFTS* urges, naval forces must “avoid a narrow definition of their capabilities.” Adequate preparations must be made to deter, confront, or defeat enemies across the entire spectrum of conflict.

Second, “maneuver at the operational level,” described as “the heart” of required capabilities, is required to exploit “a significant enemy weakness in order to deal a decisive blow” to achieve victory. Operational maneuver capabilities must be directed against an enemy’s center of gravity, that is, whatever is “essential to the enemy’s ability to effectively continue the struggle,” regardless of whether it is “a physical object (a military force, a city, a region) or a source of supplies or money.”

Third, *OMFTS* identifies the advantages afforded by naval forces in operational maneuver. It discusses the impacts of technological advances on the need for, and vulnerability of, the logistic tail of landing forces. Concluding that these two factors together with an improved command and control system “oriented toward rapid decision making” will lead to a “significant reduction of logistics infrastructure ashore," *OMFTS* argues that new capabilities will allow Marine forces "to act so quickly that the enemy will not be able to react effectively until it is too late."

To make all this happen, *OMFTS* asserts, operational planning must be improved, capabilities modernized, and intellectual underpinnings strengthened. "Significant changes" are envisioned in the way that the Marines are organized, in the way that they move between the sea and the objective, and in the way that they deal with the wide variety of missions they may undertake. Battlefield mobility, intelligence, command and control, fire support, aviation, mine counter-measures, and combat sustainment will all be enhanced. So too will doctrine, training, and education. Information Age technologies will explicitly or implicitly contribute to change and enhancement in each area.

The final chapter in this section, excerpts from *The Report of the Quadrennial Defense Review* (hereafter *QDR*), concentrates once again on providing a unified Department of Defense-wide perspective on the inter-relationships between U.S. defense policy, Information Age technologies, and the RMA. Designed as a comprehensive examination of U.S. defense requirements from 1997 to 2015, the *QDR* first discusses changes in the strategic environment and pays homage to *Joint Vision 2010*'s four new operational concepts and the idea of the "system of systems." The *QDR* then stresses that "modernization of our forces depends upon a strong backbone of command control, communications, computers, intelligence, surveillance, and reconnaissance systems (C4ISR)."

Not surprisingly, the *QDR*'s analysis of the evolving global security environment parallels those found in earlier chapters. It identifies regional dangers, the international flow of sensitive information and advanced technologies that can be used for military or terrorist purposes, transnational threats, and threats to the homeland as potential dangers. Information warfare, defined as "attacks on our infrastructure through computer-based information networks," is singled out as a specific threat. The *QDR*, like preceding chapters, expects asymmetric attacks on American forces, interests, and citizens to be a growing phenomenon. It notes that areas where the U.S. has a significant advantage such as space-based assets and C4ISR provide both greater capabilities and greater vulnerabilities.

The *QDR* argues that three elements—the abilities to shape the international security environment, respond to the full spectrum of crises, and prepare for the challenges of an uncertain future—must be the essence of U.S. defense strategy throughout the 1997-2015 period. The last of these in particular emphasizes Information Age technologies as critical components of the U.S. military's future. The *QDR* states that preparing for an uncertain future has four main parts—pursuing a focused modernization effort, exploiting the RMA, exploiting the revolution in business affairs, and developing "insurance policies"—and explicitly or implicitly stresses the importance of developing and taking full advantage of new technologies in all four.

Next, the *QDR* develops and evaluates several alternative defense policies, concluding that balancing "risk over time by sustaining sufficiently large and capable forces to shape and respond in the near and midterm, while transforming the force to meet future challenges" is the correct way to proceed. It then presents the implications of this path of action for each of five specific areas: forces and manpower, force readiness, transforming U.S. forces for the future, achieving a 21st century defense infrastructure, and defense resources.

The impacts of emerging information and communication technologies are detailed most clearly in the discussion of transforming U.S. forces for the future. Stating that "the ongoing transformation of our military capabilities…centers on developing the improved information and command and control capabilities needed to significantly enhance joint operations," the *QDR* points to information superiority as "the backbone of military innovation." It identifies five principal components of U.S. C4ISR architecture for 2010 and beyond: a "robust multi-sensor information grid providing dominant awareness of the battlespace," "advanced battle-management capabilities," "an information operations capability able to penetrate, manipulate, or deny an adversary's battlespace awareness," a "joint communications grid" that can support the above capabilities, and an "information defense system" to protect those same capabilities. The QDR next examines the ways in which these capabilities will impact dominant maneuver, precision engagement, full-dimensional protection, and focused logistics. It also discusses the way each service is approaching the RMA, often referring to service concepts and ideas put forward in *Army 2010*, *Global Engagement*, *Forward from the Sea*, and *Operational Maneuver from the Sea*.

The *QDR* also contains enlightening discussions on supporting the transformation of U.S. forces and transforming the U.S. response to asymmetric challenges. Specific programmatic changes highlighted in the first area include changes in C4ISR, JSTARS, tactical aircraft, deep strike/anti-armor weapons and munitions, ship modernization, army ground combat, and navigation. The *QDR* identifies the chief areas of asymmetric challenge as NBC weapons, terrorism, and information warfare.

Finally, the *QDR* concludes with comments from the Chairman of the Joint Chiefs of Staff. “Remarkable advances in information technology, stealth, and precision strike promise a real revolution in military affairs,” he notes. These “revolutionary technological advances,” he concludes, will combine with “new operational concepts to give us a force to dominate any future battlefield.”

The seven articles in this section, then, are unified in their assessment that a revolution in military affairs driven substantially by new and emerging information and communication technologies is well upon us. They also provide the general outlines, and at time the specific details, of how the U.S. military plans to approach and is approaching the RMA. They do not, however, always place their emphases in the same places, nor are their approaches and their terminology always identical.

Given that we are still in the infant years of the Information Age and its impact on warfare, this is to be expected. Indeed, given the uncertainties inherent in many aspects of Information Age warfare, such divergences undoubtedly provide the advantage of offering different approaches to an uncertain future.

CHAPTER 6

JOINT VISION 2010

Introduction

Joint Vision 2010 is the conceptual template for how America's armed forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. Focused on achieving dominance across the range of military operations through the application of new operational concepts, this template provides a common direction for our Services in developing their unique capabilities within a joint framework of doctrine and programs as they prepare to meet an uncertain and challenging future.

JV 2010 begins by addressing the expected continuities and changes in the strategic environment, including technology trends and their implications for our Armed Forces. It recognizes the crucial importance of our current high quality, highly trained forces and provides the basis for their further enhancement by prescribing how we will fight in the early 21st century.

The vision of future warfighting embodies the improved intelligence and command and control available in the information age and goes on to develop four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics.

Each of the operational concepts incorporates America's core strengths of high quality people and information age technological advances, builds on proven competencies, and focuses the development of future joint capabilities. Together, the application of these four concepts by robust high quality forces will provide America with the capability to dominate an opponent across the range of military operations. This Full Spectrum Dominance will be the key characteristic we seek for our Armed Forces in the 21st century….

Threads of Continuity

As we build our forces to this joint vision, there will be strong threads of continuity with the contemporary strategic and operational environment. Among these threads are American goals and interests, as well as the missions, tasks, strategic concepts, and quality of our Armed Forces.

America's Goals and Interests

America's enduring goals include: protecting the lives and safety of Americans, both at home and abroad; maintaining the political freedom and national independence of the United States with its values, institutions, and territory intact; and providing for the well-being and prosperity of the nation and its people.

These goals, in turn, generate American interests which must be protected and advanced. Our fundamental interests lie in enhancing U.S. security, promoting prosperity at home, and promoting democracy abroad….

Missions, Tasks, and Strategic Concepts of the Armed Forces

To protect our vital national interests we will require strong armed forces, which are organized, trained, and equipped to fight and win against any adversary at any level of conflict. Concurrently, we must also be able to employ these forces in operations other than war to assist in the pursuit of other important interests.

The primary task of the Armed Forces will remain to deter conflict—but should deterrence fail, to fight and win our nation's wars. In addition, we should expect to participate in a broad range of deterrent, conflict prevention, and peacetime activities. Further, our history, strategy, and recent experience suggest that we will usually work in concert with our friends and allies in almost all operations….

To ensure we can accomplish these tasks, power projection, enabled by overseas presence, will likely remain the fundamental strategic concept of our future force….Power projection from the United States, achieved through rapid strategic mobility, will enable the timely response critical to our deterrent and warfighting capabilities. Our overseas presence and highly mobile forces will both remain essential to future operations.

The Quality of Our Forces

Currently, our Armed Forces are the best trained, best equipped, and most ready force in the world. The quality of our people is unequaled at all levels of the chain of command. Leaders in each of our Services are developed through well-conceived, intensive, and long-term programs. Our equipment is first-rate and it is sustainable in all operations. Together, our personnel, leadership, and equipment are molded into exceptionally able forces through stressful training, which closely approximates wartime conditions and requirements….

Technologically superior equipment has been critical to the success of our forces in combat. This first-rate equipment, when combined with our top quality forces, has been a key element of our continuing operational successes. We must continue to ensure our soldiers, sailors, airmen, marines are fully capable of fulfilling their required tasks with equipment that is engineered to provide superior mission performance as well as safety and reliability. We must maintain a careful balance between equipping and sustaining our forces and between tooth and tail in our force structure. We must also work to assure an efficient and effective support structure and resources for all of our forces.

Dynamic Changes

Accelerating rates of change will make the future environment more unpredictable and less stable, presenting our Armed Forces with a wide range of plausible futures. Whatever direction global change ultimately takes, it will affect how we think about and conduct joint and multinational operations in the 21st century. How we respond to dynamic changes concerning potential adversaries, technological advances and their implications, and the emerging importance for information superiority will dramatically impact how well our Armed Forces can perform its duties in 2010.

The Imperative of Jointness

America’s Armed Forces are smaller than we have been in over 40 years, and we have decreased the percentage of our forces permanently stationed overseas. Faced with flat budgets and increasingly more costly readiness and modernization, we should not expect a return to the larger active forces of the Cold War period.

The American people will continue to expect us to win in any engagement, but they will also expect us to be more efficient in protecting lives and resources while accomplishing the mission successfully.... Risks and expenditures will be even more closely scrutinized than they are at present.

Simply to retain our effectiveness with less redundancy, we will need to wring every ounce of capability from every source. That outcome can only be accomplished through a more seamless integration of Service capabilities. To achieve this integration we must be fully joint: institutionally, organizationally, intellectually, and technically. Future commanders must be able visualize and create the “best fit” of available forces needed to produce the immediate effects and achieve the desired results.

Multinational Operations

It is not enough just to be joint when conducting future operations. We must find the most effective methods for integrating and improving interoperability with allied and coalition partners….

Potential Adversaries

There will continue to be states or groups that oppose or threaten American interests and values or those of our friends and allies. Our recognition of these threats and challenges will continue to drive our national security efforts.

Greater global interaction will strongly influence the nature of future threats. Wider access to advanced technology along with modern weaponry, including weapons of mass destruction (WMD), and the requisite skills to maintain and employ it, will increase the number of actors with sufficient military power to upset existing regional balances of power. Modern systems are sufficiently powerful that smaller numbers can dramatically alter the threats facing us. A number of potential adversaries may acquire the military hardware to make themselves distinctly more dangerous.

Our most vexing future adversary may be one who can use technology to make rapid improvements in its military capabilities that provide asymmetrical counters to U.S. military strengths, including information technologies. Alternatively, the high leverage associated with modern systems means that significant improvements in military capabilities can occur very rapidly, outrunning the pace of compensating political or military countermeasures.

The application of these technologies against us may also prove surprising. Our adversaries will have an independent will, some knowledge of our capabilities, and the desire to avoid our strengths and exploit vulnerabilities. We anticipate the probability of facing technological or operational surprise will increase in the period ahead.

In sum, the United States must prepare to face a wider range of threats, employing varying combinations of technology, and challenging us at varying levels of intensity.

Advancing Technology Trends

This era will be one of accelerating technological change. Critical advances will have enormous impact on all military forces. Successful adaptation of new and improved technologies may provide great increases in specific capabilities. Conversely, failure to understand and adapt could lead today's militaries into premature obsolescence and greatly increase the risks that such forces will be incapable of effective operations against forces with high technology.

Long-range precision capability, combined with a wide range of delivery systems, is emerging as a key factor in future warfare. Technological advances will continue the trend toward improved precision. Global positioning systems, high-energy research, electromagnetic technology, and enhanced stand-off capabilities will provide increased accuracy and a wider range of delivery options….

The ability to produce a broader range of potential weapons effects, from less-lethal to hard target kill, from sensor-fused to directed energy weapons, will further enhance precision capability. Advances in target effects technologies will be integrated into existing weapons and give commanders greater flexibility. These improvements will result in increasingly discrete and precise capabilities, which can achieve optimum results in both combat and other operations.

Advances in low observable technologies and the ability to mask friendly forces will also continue over the next

15 years. Signature reduction will enhance the ability to engage adversaries anywhere in the battlespace and improve the survivability of forces who employ it….Concurrently, multispectral sensing, automated target recognition, and other advances will enhance the detectability of targets across the battlespace, improving detection ranges, turning night into day for some classes of operations, reducing the risk of fratricide, and further accelerating operational tempo.

Improvements in information and systems technologies will also significantly impact future military operations by providing decision makers with accurate information in a timely manner. Information technology will improve the ability to see, prioritize, assign, and assess information. The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistic support centers will allow a greater number of operational tasks to be accomplished faster. Advances in computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations.

Forces harnessing the capabilities potentially available from this system of systems will gain dominant battlespace awareness, and interactive “picture” which will yield much more accurate assessments of friendly and enemy operations within the area of interest. Although this will not eliminate the fog of war, dominant battlespace awareness will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it.

Implications of Technological Advances on Our Armed Forces

The combination of these technology trends will provide an order of magnitude improvement in lethality. Commanders will be able to attack targets successfully with fewer platforms and less ordnance while achieving objectives more rapidly and with reduced risk. Individual warfighters will be empowered as never before, with an array of detection, targeting, and communications equipment that will greatly magnify the power of small units. Strategically, this improvement will enable more rapid power projection and reduced logistics tails. Operationally, within the theater, these capabilities will mean a more rapid transition from deployment to full operational capability. As a result, we will improve our capability for rapid, worldwide deployment while becoming even more tactically mobile and lethal.

The implications of this increased lethality for overall for e structure requirements are unclear….[M]any military missions will require occupation of the ground, and intensive physical presence. For these missions the promises of technology are less certain, especially in environments such as cities or jungles.

During all operations, advanced technologies in the hands of an adversary will increase the importance of force protection at all echelons. Any efficiencies garnered by our offensive systems must be underwritten by appropriate redundancies to safeguard against unanticipated technological, strategic, or operational surprises.

Adaptations to this increasingly lethal battlespace will be warranted. These adaptations are likely to take the forms of increased stealth, mobility, dispersion, and pursuit of a higher tempo of operations among elements within the battlespace….

Greater mobility and increased dispersion will, in turn, require additional communications and coordination capabilities since the synchronization of these dispersed elements will become even more important. Fortunately, the technology for this improved systems integration is at hand.

The implications of improved systems integration are both profound and complex. New technologies will allow increased capability at lower echelons to control more lethal forces over larger areas, thus leveraging the skills and initiative of individuals and small units. These capabilities could empower a degree of independent maneuver, planning, and coordination at lower echelons, which were normally exercised by more senior commanders in the past. Concurrently, commanders at higher echelons will use these technologies to reduce the friction of war and to apply precise centralized control when and where appropriate.

Even for higher level commanders, the accelerated operational tempo and greater integration requirements will likely create a more stressful, faster moving decision environment. Real-time information will likely drive parallel, not sequential, planning and real-time, not prearranged, decision making. The optimal balance between centralized and decentralized command and control will have to be carefully developed as systems are brought into the inventories.

Emerging Importance of Information Superiority

Throughout history, gathering, exploiting, and protecting information have been critical in command, control, and intelligence. The unqualified importance of information will not change in 2010. What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology. While the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact.

Sustaining the responsive, high quality data processing and information needed for joint military operations will require more than just an edge over an adversary. We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information superiority will require both offensive and defensive information warfare (IW). Offensive information warfare will degrade or exploit an adversary's collection or use of information. It will include both traditional methods, such as a precision attack to destroy and adversary's command and control capability, as well as nontraditional methods such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers.

There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. Defensive information warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead. Traditional defensive IW operations include physical security measures and encryption. Nontraditional methods will range from antivirus protection to innovative methods of secure data transmission. In addition, increased strategic level programs will be required in this critical area.

Conduct of Joint Operations

Our forces have been largely organized, trained, and equipped to defeat military forces of our potential adversaries. Direct combat against an enemy's armed forces is the most demanding and complex set of requirements we have faced. Other operations, from humanitarian assistance in peacetime through peace operations in a near hostile environment, have proved to be possible using forces optimized for wartime effectiveness.

Technological advances will magnify the advantages provided by our high quality force. The promise provided by these technologies is best viewed from an operational perspective. In the past, our capabilities often required us to physically mass forces to neutralize enemy power. The time needed to build up and employ massed combat forces, including the platforms, weapons, and associated logistics, required to achieve success resulted in military operations that were largely sequential in nature and tactics which too often saw ground, maritime, and air forces massed in time and space.

By 2010, we should be able to change how we conduct the most intense joint operations. Instead of relying on massed forces and sequential operations, we will achieve massed effects in other ways. Information superiority and advances in technology will enable us to achieve the desired effects through the tailored application of joint combat power. Higher lethality weapons will allow us to conduct attacks concurrently that formerly required massed assets, applied in a sequential manner. With precision targeting and longer range systems, commanders can achieve the necessary destruction or suppression of enemy forces with fewer systems, thereby reducing the need for time-consuming and risky massing of people and equipment. Improved command and control, based on fused, all-source, real-time intelligence will reduce the need to assemble maneuver formations days and hours in advance of attacks. Providing improved targeting information directly to the most effective weapon system will potentially reduce the traditional force requirements at the point of the main effort.

…in all operations technological advances and our use of information will give our warfighters at the individual, crew, and small unit levels major qualitative advantages over potential adversaries. Our forces will be able to sense danger sooner. They will have increased awareness of the overall operational environment, including the situation of friendly forces, allowing them to make better decisions more rapidly. They will have an enhanced ability to produce a range of desired effects by bringing together the correct mix of assets at the place and time most favorable to success. When tied to a more rapid resupply, reinforcement, and reengagement capability, they will be better able to provide the best response at less risk to themselves, based on the mission objectives and circumstances of the battlespace. Whether operating from dispersed locations or in close proximity to each other, the confidence of each individual warfighter or crew will be bolstered by enhanced connectivity to comrades, supporting elements, and higher commands.

In sum, by 2010, we should be able to enhance the capabilities of our forces through technology. This will, in turn, expand our greatest advantage: the adaptability, initiative, teamwork, and commitment of our people at every level.

To exploit the enormous potential of technology, we must develop in a systematic manner the full range of required enhancements. This process must begin with a new conceptual framework for operations.

The basis for this framework is found in the improved command, control, and intelligence which can be assured by information superiority. These are the most straightforward applications of much of the new technology; however, the full impact of these technologies is more profound. Enhanced command and control, and much improved intelligence, along with other applications of new technology will transform the traditional functions of maneuver, strike, protection, and logistics. These transformations will be so powerful that they become, in effect, new operational concepts: dominant maneuver; precision engagement; full dimensional protection; and focused logistics. These operational concepts will provide our forces with a new conceptual framework.

New Operational Concepts

Dominant maneuver will be the multidimensional application of information, engagement, and mobility capabilities to position and employ widely dispersed joint air, land, sea, and space forces to accomplish the assigned operational tasks. Dominant maneuver will allow our forces to gain a decisive advantage by controlling the breadth, depth, and height of the battlespace….

Dominant maneuver will require forces that are adept at conducting sustained and synchronized operations from dispersed locations. They must be able to apply overwhelming force in the same medium and create asymmetric advantages by attacking cross-dimensionally, such as air or sea against ground or ground and sea against air defenses. These forces must have the ability to outpace and outmaneuver the enemy. Current systems, enhanced by information superiority, will provide a clearer picture of enemy and friendly locations. Information superiority will also allow joint commanders to coordinate widely dispersed units, receive accurate feedback, and execute more demanding, higher precision requirements. Increasingly lethal direct and indirect fire systems, with longer ranges and more accurate targeting, will increase the punch of these forces as they maneuver….

Altogether, the organizational concept of dominant maneuver is a prescription for more agile, faster moving joint operations, which will combine air, land, and maritime forces more effectively to deliver decisive combat power.

Precision engagement will consist of a system of systems that enables our forces to locate the objective or target, provide responsive command and control, generate the desired effect, assess our level of success, and retain the flexibility to reengage with precision when required. Even from extended range, precision engagement will allow us to shape the battlespace, enhancing the protection of our forces.

Information operations will tie together high fidelity target acquisition, prioritized requirements, and command and control of joint forces within the battlespace. This will provide a greater assurance of delivering the desired effect, lessen the risk to our forces, and minimize collateral damage.

Precision engagement will build on current U.S. advantages in delivery accuracy and low observable technologies. It will use a wide variety of means, including very accurate aerial deliveries or air drops, discriminate weapon strikes, and precise, all-weather stand-off capability. Enhance jointness will ensure greater commonality between Service precision engagement capabilities and provide future joint commanders with a wider array of responsive, accurate, and flexible options.

[Full-dimensional protection will] protect our own forces from the very technologies that we are exploiting. Unless we provide an adequate measure of protection for our forces, these new operational concepts will be highly vulnerable to disruption….The primary prerequisite for full-dimensional protection will be control of the battlespace to ensure our forces can maintain freedom of action during deployment, maneuver and engagement, while providing multi-layered defenses for our forces and facilities at all levels….

Full dimensional protection will be built upon information superiority which will provide multidimensional awareness and assessment, as well as identification of all forces in the battlespace. Information warfare will support this effort by protecting our information systems and processes, while denying an adversary the similar capabilities.

Upon this information base, we will employ a full array of active and passive measures at multiple echelons. Active measures will include battlespace control operations to guarantee the air, sea, space, and information superiority that is needed to gain the degree of control to accomplish the assigned tasks….

Passive measures will include the inherent protection provided by information superiority and dispersal to increase our warning of attacks. Operational dispersal will further reduce risks to our forces. New sensors and information dissemination systems will be deployed to detect chemical or biological attack at great range and provide warning to specific units that may be affected….

Most importantly, these active and passive measures will be combined to provide a more seamless joint architecture for force protection, which will leverage the contributions of individual Services, systems, and echelons. The result will be improved freedom of action for friendly forces, and better protection at all echelons against precision attack, weapons of mass destruction, and other conventional or non-conventional systems.

…*Focused logistics* will be the fusion of information, logistics, and transportation technologies to provide rapid crisis response, to track and shift assets even while en route, and to deliver tailored logistics packages and sustainment directly at the strategic, opertional, and tactical level of operations. It will be fully adaptive to the needs of our increasingly dispersed and mobile forces, providing support in hours or days versus weeks. Focused logistics will enable joint forces of the future to be more mobile, versatile, and projectable from anywhere in the world.

Logistic functions will incorporate information technologies to transition from the rigid vertical organizations of the past….Information technologies will enhance airlift, sealift, and pre-positioning capabilities to lighten deployment loads, assist pinpoint logistics delivery systems, and extend the reach and longevity of systems currently in inventory. The combined impact of these improvements will be a smaller, more capable deployed force. It will require less continuous support with a smaller logistics footprint, decreasing the vulnerability of our logistics lines of communication.

Full Spectrum Dominance

Each of these new operational concepts will reinforce the others and will allow us to achieve massed effects in warfare from more dispersed forces. This synergy will greatly enhance our capabilities in high intensity conventional military operations.

However, the synergy of these four concepts transcends intense conventional warfighting. Without overspecialization, the development of these new operational concepts has great potential to fulfill more effectively the full range of tasks assigned to us. That is, taken together, these four new concepts will enable us to dominate the full range of military operations from humanitarian assistance, through peace operations, up to and into the highest intensity conflict.

Information superiority will provide a commander with enhanced awareness of his area of responsibility, whether his objective is to close with and engage an adversary or render assistance in a humanitarian operation. Surveillance, reconnaissance, and knowledge of the precise location of dispersed friendly forces with the ability to direct effectively their efforts are applicable for all military tasks.

Likewise, the tactical mobility required for dominant maneuver which enables our forces rapidly to move into position to overwhelm an enemy will also allow commanders to place forces in positions of control in counterdrug, counterterrorism, or peacekeeping operations. Precision engagement capabilities designed for warfighting tasks will also enable greater discrimination in the application of force against an emerging threat during peace enforcement operations. Full-dimensional protection will allow freedom of action for our forces and limit their vulnerability during combat and noncombat operations. Focused logistics will ensure delivery of the precise amount and types of supplies required for our joint forces to succeed in combat or noncombat operations.

Although the positive implications for enhancing our capabilities across the range of military operations seems obvious, we cannot assume that all new concepts will be equally valuable in all operations. In intensive combat, target destruction may be essential in the early engagements of an operation, but extensive physical presence may later be necessary to accomplish the assigned mission. This presence may be required to fully neutralize enemy forces, deal with prisoners and potentially hostile populations, or otherwise assure that success in attacking targets is followed through to achieve the overall objectives of the operation. For noncombat operations, physical presence will likely be even more important. Thus, we must ensure that capturing the new technologies does not overspecialize the force; we must retain balanced and sustainable capabilities. We recognize that, regardless of how sophisticated technology becomes, the individual warfighter's judgement, creativity, and adaptability in the face of highly dynamic situations will be essential to the success of future joint operations. The human element is especially important in situations where we cannot bring our technological capabilities fully to bear against opponents who seek to nullify our technological superiority by various means. In these cases, our success will depend, as it has historically, upon the physical, intellectual, and moral strengths of the individual soldier, sailor, airman, and marine—especially their adaptability in the face of the unexpected.

Critical Considerations

To sustain the Armed Forces and instill these new operational concepts will require high quality people—the key ingredient for success. The judgement, creativity, and fortitude of our people will remain the key to success in future joint operations. Turning concepts into capabilities requires adapting our leadership, doctrine, education and training, organizations, and material to meet the high tempo, high technology demands posed by these new concepts.

Dedicated, High Quality People

Thus, recruiting and retaining dedicated high quality people will remain our first priority. Only a force that has the courage, stamina, and intellectual ability to cope with the complexity and rapid pace of future joint operations will have the capability to achieve full spectrum dominance.

We cannot expect risk-free, push-button style operations in the future. Military operations will continue to demand extraordinary dedication and sacrifice under the most adverse conditions. Some military operations will require close combat on the ground, at sea, or in the air. The courage and heart of our soldiers, sailors, airmen, and marines will remain the foundation of all that our Armed Forces must do.

Innovative Leadership

The dynamic nature of joint operations in the 21st century battlespace will require a continued emphasis on developing strong leadership skills. While we must do everything possible to leverage the power of advanced technologies, there are inherent limitations. Confronting the inevitable friction and fog of war against a resourceful and strong minded adversary, the human dimension including innovative strategic and operational thinking and strong leadership will be essential to achieve decisive results. Effective leadership provides our greatest hedge against uncertainty….

Joint Doctrine

As we change the way we fight, joint doctrine will remain the foundation that fundamentally shapes the way we think about and train for joint military operations. Joint doctrine is a critical ingredient for success because the way in which leaders think and organize their forces will be as important as the technology we use to conduct future joint operations. Future joint doctrine must articulate the process required for successful joint planning but must be flexible enough to serve as a broad framework to guide our forces in joint and multinational operations. It is the key to enhanced jointness because it transforms technology, new ideas, and operational concepts into joint capabilities….

Joint Education and Training

Our education and training programs must prepare joint warriors to meet the challenges of the future battlespace. These programs must emphasize employment of new technologies and achieving the operational concepts outlined in this vision….

Agile Organizations

In order to make optimum use of the technologies and operational concepts discussed earlier, we must carefully examine the traditional criteria governing span of control and organizational layers for the Services, commands, and Defense agencies. We will need organizations and processes that are agile enough to exploit emerging technologies and respond to diverse threats and enemy capabilities. As we move forward, we may require further reductions in supervision and centralized direction.

All organizations must become more responsive to contingencies, with less “startup” time between deployment and employment….

Enhanced Material

Since most of the platforms expected to be in service in 2010 are already designed or operational, we will emphasize high leverage, leading edge technology enhancements to increase our capabilities. We will also place greater emphasis on common usage between Services and increase interoperability among the Services and multinational partners.

We will need a responsive research, development, and acquisition process to incorporate new technologies. This process must leverage technology and management innovations originating in the private sector through responsive access to commercial developments.

Implementing Joint Vision

We must proceed with implementing *Joint Vision 2010* in a way that captures the promise of these new concepts while sustaining our readiness and flexibility through every step of this evolution….

As we implement this vision, affordability of the technologies envisioned to achieve full spectrum dominance will be an important consideration. While we anticipate that some significant improvements in capability may be gained economically, for example through dual-use technologies for C4I, others will be more difficult to achieve within the budget realities that exist today and will exist into the next century. We anticipate the need to be selective in the technologies we choose, and thus expect continuing assessment and adjustments for affordability as well as for other lessons learned during the implementation process.

Achieving the full promise of this vision will largely depend on how well we structure our defense program. We will have to make hard choices to achieve the tradeoffs that will bring the best balance, most capability, and greatest interoperability for the least cost. Ultimately, we will have to measure continuously the affordability of achieving full spectrum dominance against our overarching need to maintain the quality of our forces, their readiness, and the force structure needed to execute our operational tasks between now and the year 2010.

As we implement this vision, we must acknowledge that strong leadership, warfighting skill, and innovative thinking will be central to developing the detailed requirements and decision points. Our organizational climate must reward critical thinking, foster the competition of ideas, and reduce structural or cultural barriers to innovation. Both in peace and war, the creative talents of our men and women provide us a critical advantage over those who would consider challenging us or our allies.

Conclusion

Today, America’s Armed Forces are the world standard for military excellence and joint warfighting. We will further strengthen our military capabilities by taking advantage of improved technology and the vitality and innovation of our people to prepare our forces for the 21st century.

Joint Vision 2010 creates the template to guide the transformation of these concepts into joint operational capabilities. It serves as the basis for focusing the strengths of each individual Service or component to exploit the full array of available capabilities and allow us to achieve full spectrum dominance. It will also guide the evolution of joint doctrine, education, and training to assure we will be able to achieve more seamless joint operations in the future.

As we pursue this vision, we must remain mindful of our responsibilities: to prevent threats to our interests from emerging, deter those that do, and defeat those threats by military force if deterrence fails. In 2010, we will meet these responsibilities with high quality people and leaders, who are trained and ready for joint operations and able to exploit high technology equipment. Even during a time of unparalleled technological advances we will always rely on the courage, determination, and strength of America’s men and women to ensure we are persuasive in peace, decisive in war, and preeminent in any form of conflict.

CHAPTER 7

ARMY VISION 2010

Introduction

Army Vision 2010 is the blueprint for the Army's contributions to the operational concepts identified in *Joint Vision 2010*. It is the conceptual template for how the United States Army will channel the vitality and innovation of its soldiers and civilians and leverage technological opportunities to achieve new levels of effectiveness as the land component member of the joint warfighting team.

Joint Vision 2010 provides a coherent view of the future and the implications for joint operations expressed in terms of emerging operational concepts. *Army Vision 2010* focuses on the implications of that environment for the fundamental competency the Army contributes to joint operations—the ability to conduct prompt and sustained operations on land throughout the entire spectrum of crisis. It identifies the operational imperatives and enabling technologies needed for the Army to fulfill its role in achieving full spectrum dominance.

Army Vision 2010 also serves as a linchpin between Force XXI, the Army's ongoing process to manage change and advance into the 21st century with the most capable Army in the world, and the Army After Next (AAN), the Army's emerging long-term vision. It is the necessary and intermediate objective en route to the next generation of strategies, soldiers, structures, and systems. While *Army Vision 2010* strives to visualize developing concepts and technologies to improve capabilities circa 2010, the AAN process stretches to conceptualize the geostrategic environment 30 years into the future. Force XXI, *Army Vision 2010*, and AAN work collaboratively to identify the types of capabilities and areas of technology applications that will accommodate their respective environments and the implications for Doctrine, Training, Leader Development, Organization, Materiel, and Soldiers. Force XXI, *Army Vision 2010*, and AAN establish a continuum of orderly change, assuring a disciplined approach to meeting the challenges of an uncertain future and maximizing the innovativeness of the military, academia, and industry.

As the Army progresses along this continuum, aligning its vision with *Joint Vision 2010*, it will serve us well to keep in mind why the Nation has an army, the values that distinguish our soldiers, and the bond between the Army and the Nation- these things will not change. They are the essence of our being, and neither the geostrategic environment nor technology will break the common threads that tie yesterday’s soldiers at Valley Forge to today’s soldiers on the demilitarized zone in Korea, or in Bosnia, or elsewhere around the globe, to tomorrow’s soldiers in the 21st century.

Why an Army—Yesterday, Today, and Tomorrow

To Fight and Win the Nation's Wars

The power to deny or to destroy is possessed by each of the military Services. The contribution of land forces to the joint warfight is the power to exercise direct, continuing, and comprehensive control over land, its resources, and its peoples. It is this direct, continuing, and comprehensive control over land, resources, and people that allows land power to make permanent the otherwise transitory advantages achieved by air and naval forces.

To Provide a Range of Military Options Short of War—Military Options Other Than War (MOOTW)

Land forces perform important, and largely unique, functions besides denial and destruction. Because of their versatility, they are distinctly capable of making contributions in a sustained and measured way across the broadest array of national requirements.

Primary among these contributions is the role land forces play in support of preventive defense. Through peacetime engagement, land forces are active and dominant players in preventive defense activities ranging from nation building to military-to-military contacts. Through their presence, they provide a unique capability to impart American/democratic values as they interact with nations' armies and peoples to favorably shape the world environment and help keep potential dangers to our security from becoming full-blown threats.

They are the force that protects and controls populations, restores order, and facilitates the transition from hostilities to peace. It is through this dimension of influence that the land force component, the Army, serves to strengthen the Nation’s position in security and foreign policy, in negotiating treaties, in dealing with foreign governments, and in establishing alliances.

The land component is also the force of choice to respond to natural and man-made disasters, assist communities during civil disturbances, and perform civic action/nation-building projects as required. In a dynamic and unpredictable geostrategic environment, the U.S. Army provides a full range of choices to the Nation and a hedge against uncertainty—a unique asset, a national asset.

To Deter Aggression

The threat of employing fully trained, highly motivated military forces equipped with modern, powerful warfighting systems serves as a credible deterrent to adversaries who might otherwise perceive the risk of conflict worth the spoils of war. The forward stationing of land forces on foreign soil identifies regions of U.S. vital interests and signals the highest degree of commitment that these interests will be protected. The deployment of military forces in times of crisis commits the prestige, honor, and resolve of the Nation. The deployment of land forces is the gravest response that can be made, short of war, to demonstrate the national will to prevent conflict.

The Army's Enduring Values—Yesterday, Today, and Tomorrow

The Army is more than an organization; it is an institution with a unique and enduring set of values. The Army instills these values in its soldiers and civilians, the men and women who are the Army. The terms the Army uses to articulate its values—honor, integrity, selfless service, courage, loyalty, duty, and respect—inspire the sense of purpose necessary to sustain soldiers in combat and help resolve the ambiguities of military operations where war has not been declared. Leaders of character and competence live these values. They build an Army where people do what is right, treat others as they themselves want to be treated, and can be all they can be….

The Army-Nation Bond—Yesterday, Today, and Tomorrow

Committing the Army commits the Nation. Committing the United States Army makes a strong statement that friends and adversaries alike cannot misinterpret. No other single gesture so clearly demonstrates the ultimate commitment of the U.S. to a particular outcome as placing American soldiers in harm's way. The Army's strength always has been, and always will be, the American soldier. Soldiers are the Army. The Army makes the most significant investment it can make to the Nation's security by properly training, equipping, and supporting our soldiers.

The Geostrategic Environment and Its Implications for Land Forces

The Land Force—The Versatile Force

With the end of the Cold War, a prominent theory arose that there would no longer be a need for large land forces, that power projection and national military strategy could primarily be carried out through precision strikes using technologically advanced air and naval forces. This "standoff" approach would reduce the level of U.S. involvement and commitment and thus the requirement for large land forces. Reality proved that theory to be invalid.

During the 40 years from 1950 to the collapse of the Soviet Union, the Army conducted 10 notable deployments. Since 1990, in the short span of 6 years, we have deployed 25 times—an increase in missions by a factor of 16. This new paradigm reflects the significance of land forces in supporting the National Security Strategy of engagement and enlargement.

What will the future hold? The significance of land power as the force of decision will continue to rise for several reasons. First, most future operations will occur on the lower and middle portions of the continuum of military operations ranging from disaster relief to global war, where land forces provide unique and essential capabilities, the most options, and the most useful tools. These types of operations require the commitment of U.S. land forces to establish leadership and to enable our allies and coalition partners. They call for soldiers on the ground, directly interfacing with the civilians and/or military involved in the crisis. Should the Nation's military be called to take on additional, nontraditional missions in support of a broadened National Security Strategy, the utility of land forces will increase even more.

The second reason for the rise in significance of land forces is their direct relevance to the National Military Strategy's strategic enablers: overseas presence and power projection. Without a doubt, all Services fulfill critical functions in support of these two enablers; however, two unique characteristics apply to land forces. First, they provide the most visible, sustained foreign presence—on the ground, 24 hours a day, person-to-person…cooperating, sharing risks, representing America. Second, as illustrated in the accompanying chart, land forces not only provide the most flexible and versatile capabilities for meeting CINC force requirements, from humanitarian assistance to combat operations, but constitute the highest percentage of the committed joint force.

Third, land forces are important to U.S. international credibility. The recent past provides a convincing example in the NATO deployment to Bosnia. Recognizing the substantial participation of U.S. air and naval forces over the past 3 years to support the naval blockade, air supply operations, and a no-fly zone in the Balkans, the NATO peace plan ultimately required a large, visible contingent of U.S. ground troops.

Fourth, U.S. land forces are most suitable for supporting the military's contribution to peacetime engagement and interaction with foreign military forces. The overwhelming majority of military forces throughout the world are predominantly armies. Few countries have the need or resources to maintain significant air or naval forces. Military engagement in these countries normally means army-to-army contact. Moreover, we see this phenomenon gaining importance. As former army officers ascend to key positions in their national leadership structures, the Army's cooperative ties will increase in significance and continue to provide U.S. leadership with valuable contributions to international engagement.

However, while cognizant of the increased demand for land forces at the lower end of the contingency spectrum in the near term, we must remain vigilant of the fundamental role of the Army—to fight and win the Nation's wars as the land component of the joint force.

While the threat of global war may be diminishing, the world continues to be a dangerous place, especially in those regions where traditional conflict is an acceptable means of achieving national interests, specifically the Euro-Middle East and the Asian Arc regions. Within each of these regions lie numerous nation states on their way to participating democracies and/or advanced economies. In this "transitional zone," the inherent instability in the region could evolve into actual war as once dominant states perceive an unfavorable shift in power relative to their neighbors. These states, while less capable militarily than wealthy democracies, have access to the most advanced military technology. This phenomenon creates a new danger in the future, i.e., conflict with a nation having a very sophisticated and asymmetric capability.

The motivations and prosecution of these wars will be varied. In the Euro-Middle East region (west of the Urals to the Persian Gulf to the North Atlantic), oil and radical fundamentalism serve as potential catalysts to armed conflict and will continue to do so into the foreseeable future. In the Asian Arc region (stretching from Petropavlosk to India/Pakistan), resides one half of the world's population. In that region the shortage of food and arable land will pose increasingly demanding challenges in the next century. China alone has 1.2 billion people, making the U.S. population, by comparison, "right of the decimal point." Here also, war will continue to be viewed as a viable means of achieving or protecting their national interests. The conduct of war will be equally dissimilar. The general nature of combat notwithstanding, the very essence of conflict prosecuted by nations in the Asian Arc region is unlikely to be the same as that prosecuted by nations in the Euro-Middle East region. Disparate cultures, terrain, and climates will drive significant differences in their force structures, tactics, and warfighting strategies.

Collectively, the geostrategic environment, the near-term increased demand for operations on the lower end of the spectrum of crisis, and the continuing requirement to prepare to win the Nation's wars suggest a redefinition of general missions for the military. These missions can be categorized into seven general areas: Defending or Liberating Territory, Punitive Intrusion, Conflict Containment, Leverage, Reassurance, Core Security, and Humanitarian.

FULL SPECTRUM CAPABILITIES

Missions	Required Army Capabilities
Defending or Liberating Territory	
MRC	HVY/LT/SOF
LRC	HVY/LT/SOF
Punitive Intrusion	
Counter Drug	LT/SOF/TECH
Counter Terrorism	LT/SOF
Counter Proliferation	SOF
Conflict Containment	
MOOTW	HVY/LT/SOF
Leverage	
TMD	TECH
Space Applications	TECH
C4I Systems Integration	TECH
Battlefield Awareness	TECH
Reassurance	
Presence	HVY/LT/SOF
Core Security	
NMD	TECH
Counter Drug	HVY/LT/SOF/TECH
Illegal Immigration	LT/SOF
Crime in the Streets	LT/SOF
Humanitarian	
Disaster Relief	LT/SOF
Population Evacuation	HVY/LT/SOF
Refugee Protection	HVY/LT/SOF
Cooperation, Exchanges, Training	HVY/LT/SOF

Within these seven mission areas lie numerous crises that the military may be tasked to respond to in the years ahead. While the magnitude and frequency of these crises are unpredictable, it is certain that the full spectrum of Army capabilities will be required to contribute to each of these general missions at some time in the next century.

Technology will also play a unique role in defining capabilities as we look to the future. Consequently, we must continue to leverage the superiority of the U.S. industrial base and maintain a decisive advantage across the full range of these mission areas. While at the moment we have technological superiority, advanced warfighting capabilities are available to any nation with the means to procure them. Not coincidentally, the most active customers lie in the "transitional zone."

Implications

[This analysis leads to several implications:]

- We must have a military capable of deterring or defeating an emerging competitor.

- A regional focus is required for rapid response to crises in the "transitional zone," where the Nation's vital interests are most at risk.

- The frequency of demands for land forces will increase as the Army is called upon to support peacetime engagement activities, i.e., multilateral military exercises, training, military-to-military exchanges, as well as crises on the lower end of the continuum, e.g., humanitarian relief, peacekeeping, peacemaking, etc.

- Technology will play an important role in enabling full-spectrum operations.

These implications suggest two primary axes: a regional focus for the traditional role of our Army and a balanced force mix to ensure "full-spectrum capability" to execute the roles and missions most likely to be levied on land forces as we enter the next century. Each of these axes will require leveraging technology to ensure swift victory with minimal casualties across the continuum of crisis.

Army Vision 2010 provides the directional azimuth for these parallel axes and assists in sizing, organizing, and equipping the Army, and in developing the doctrine for land force operations in support of *Joint Vision 2010*. Leader development and training programs will be continually refined to keep the Army prepared to execute these full-spectrum operations as the force of decision.

The Way Ahead

Historically, we have not had the exact Army we needed when we needed it. Still, we were never truly wrong because we built an Army with a core set of capabilities and infused it with the agility and flexibility to adapt to domestic or international demands as they arose. The future will demand more…the modality of agility will be even more essential to our ability to adapt to a dynamic strategic environment. We will need to continuously leverage technology to ensure our force has the requisite advantage to preclude conflict if possible, but to win decisively if necessary, and to leverage the capabilities of our allies and coalition partners. In the aggregate, we must "lighten up the heavy forces and heavy up the capabilities of the light forces." Ultimately, we must always be assured of victory and certain we will never be forced to negotiate from a position of weakness.

At the very heart of this strategy is our continuing commitment to a Total Quality Force. The challenging global security environment, the complexity of emerging technologies, and the diverse missions being assigned to the Army will require men and women of intelligence and dedication, in the active and reserve components, who are able to adapt quickly to the missions at hand. Reductions in the active force have made the reserve component even more essential to meeting the Nation's needs across the full spectrum of operations, from disaster relief to war. They are equal partners in meeting the challenges of the 21st century and must be trained and equipped with modern, compatible equipment to perform assigned missions with their active duty counterparts and coalition partners. Consequently, maintaining quality soldiers and civilians throughout the Total Force is our top priority. To sustain the essential contributions soldiers and civilians make, quality of life programs, a steady flow of promotions, and schooling opportunities must continue throughout their careers.

As we move into the 21st century, we will remain true to our heritage. At the same time we will adapt our doctrine, force structure, modernization program, training, and leader development to accommodate the evolving world environment and ensure Army capabilities are integrated with those of other Services and our allies to achieve maximum operational effectiveness. We will move toward *Army Vision 2010* with a common view of the future. The geostrategic environment and *Joint Vision 2010* provide the construct for that common view and the guideposts to the 21st century.

Achieving Full-Spectrum Dominance

…Land component operations in 2010 will be fully integrated with those of joint, multinational, and nongovernmental partners. Recent experience reminds us that Army operations have never been and will never be independent. From initial mission receipt through deployment, operations, and transition to follow-on operations, Army elements will execute their responsibilities through a deliberate set of patterns of operation. These patterns are not phases, nor are they sequential. They serve to focus the many tasks armies have always performed in war and other military operations. The patterns are: Project the Force, Protect the Force, Shape the Battlespace, Decisive Operations, Sustain the Force, and Gain Information Dominance. Five of these patterns of operation align precisely with the *Joint Vision 2010* operational concepts of Dominant Maneuver, Precision Engagement, Focused Logistics, and Full Dimensional Protection. The sixth, Gaining Information Dominance, is fundamental to each of the other five Army patterns of operation as well as each of the operational concepts in *Joint Vision 2010*. The succeeding paragraphs identify the interrelationship between the Army's patterns of operation and the operational concepts in *Joint Vision 2010*, as well as the enablers and technologies the Army will pursue to fulfill its role in achieving full-spectrum dominance as the land component member of the joint team.

Dominant Maneuver

Dominant Maneuver will be the multidimensional application of information, engagement, and mobility capabilities to position and employ widely dispersed joint air, land, sea, and space forces to accomplish assigned operational tasks.

For the land component, dominant maneuver consists of two elements: strategic and operational. Strategic maneuver equates to the Army's requirement to project the force. It initiates the process of creating an image in the mind of an adversary of an unstoppable force of unequaled competence. American land forces will begin this process of moral domination from points of embarkation around the world just as surely as winning forces have done throughout history. Time and distance change the geometry, but the principles and effects of simultaneity are the same.

Augmented with critical equipment pre-positioned where the need is most likely, air and naval components of the joint force will commence transport of a versatile, tailorable, modular Army within hours of the decision to deploy. This power projection force will be equipped with lighter, more durable, multipurpose warfighting systems, thus reducing the amount of lift required, as well as the size and complexity of the logistics tail needed to sustain the force.

Strategic Maneuver

Concepts

Rapid Tailoring

CONUS-based…Rapidly Deployable

Prepositioned Equipment and Forward Presence

Deploy Directly to Combat

Part of Joint/Combined/Interagency Force

Enablers

Modular Organization

Equipment Prepositioned

Army War Reserve Prepositioned Stock

En Route Battle Command and Mission Rehearsal

Total Asset Visibility

Joint, Lethal, Early Entry Forces

Global, Broadcast Network

Strategic Lift

Technologies

Global Cellular Communications

Smart Pagers

Intelligence Preparation of the Battlefield (IPB) En Route

Lighter Materials

Simulations

Operational maneuver, the other element of dominant maneuver, equates to decisive operations. Decisive operations force the enemy to decide to give in to our will. They are inextricably linked to shaping the battlespace and precision engagement in that decisive operations are vastly enhanced by the precision fires, precise information, and precise detection capabilities inherent to precision engagement. In combat operations, decisive operations are defined in terms of victories in campaigns, battles, or engagements. In other military operations, decisive operations are defined in terms of accomplishing the military objectives (free elections in Haiti or the absence of war in Bosnia are examples). Within the patterns of operation, decisive operations are the means of achieving success. The Army, armed with situational understanding, will conduct decisive operations by positioning combat power throughout the battlefield. This unique capability—to exercise direct, continuing, and comprehensive control over land, its resources, and people—is the essence of the Army's contribution to the joint force in winning the Nation's wars.

Modern technologies will exploit situational understanding phenomena to enable tailored, still undefined combat organizations to task organize quickly and fight dispersed with extraordinary ferocity and synchronization. Fused inputs from manned and unmanned sensors (including satellites) will provide unprecedented battlefield situational understanding to depths well beyond the horizon. Significant advances in avionics, weaponry, vehicle mobility, stealth, survivability, and communication technologies will make the land force truly the force of decision on the 21st century battlefield.

Operational Maneuver

Concepts

Mass Effects, Not Forces

Simultaneous, Brief, Violent

Attacks in Multiple Directions

Attack, Disengage, Reorganize, Reattack

Enablers

Battle Command on the Move

Information Dominance

Lethality at Extended Ranges

Precision Systems and Munitions

Simultaneous Application of Joint Capabilities

Mobility, Speed, Agility

Technologies

Stealth

Manned Sensors

Unmanned Sensors

Advanced Avionics

High-Speed Vehicular Mobility

Information Warfare Technologies

Horizontal Technology Integration

Digitization

Simulations

Precision Engagement

Precision engagement will consist of a system of systems that enables joint forces to locate the objective or target, provide responsive command and control, generate the desired effect, assess the level of success, and retain the flexibility to reengage with precision when required.

Precision Engagement

Concepts

Dominate Expanded Multidimensional Battlespace

Simultaneity

Destroy Enemy Key Capabilities and Freedom of Action Early

Preserve Friendly Freedom of Action

Create Windows of Capabilities Overmatch

Influence Enemy Perceptions

Enablers

Dynamic Obstacles

Sensor-Shooter Links

Simultaneous Application of Joint Capabilities

Increased Lethality at Extended Ranges

Precision Systems and Munitions

Demonstrations and Feints, Psychological Operations (PSYOPS), Media Relations, Deception

Technologies

Artificial Intelligence (AI) Algorithms

Signature Cataloging

Combat ID

Onboard Sensor Processing

Brilliant Munitions

Shaping the battlespace sets the conditions for success—it is directly linked with decisive operations. Together they allow the force to overcome the enemy's center of gravity and result in the total takedown of an opponent. For land forces, shaping the battlespace is far more than precision strike which, as a lone function, is nothing more than 21st century attrition warfare. Shaping the battlespace is the unambiguous integration of all combat multipliers—feints, demonstrations, limited attacks, command and control warfare (C2W), mobility/countermobility, deception, and all available fires—with the scheme of maneuver to achieve simultaneity and thus overwhelm the enemy. It sets conditions in terms not only of what we do to the enemy, but also how we posture the friendly force and take advantage of the operational environment (terrain, weather, and infrastructure).

Shaping the battlespace begins with early Intelligence Preparation of the Battlefield (IPB). IPB supports identification of the enemy's main effort and enables the Land Component Commander (LCC) to decide on those high-value targets that will facilitate his scheme of maneuver, prioritize and sequence collection assets to detect and track those targets, and assign the appropriate weapon system to deliver the correct munitions to destroy those targets where and when he chooses.

Shaping the battlespace will be facilitated primarily by sharing "real time" information among all Services, allies, and coalition partners. This process will be accomplished by effectively exploiting information age technologies that permit: isolating, tagging, and tracking of the most fleeting enemy forces and targets with precision; processing and fusing multiple sources of information from all involved components; and employing the proper force, munitions, or energy before the target is lost. Immediate and accurate battle damage assessment will facilitate re-engagement. As future joint forces combine processes to make virtually any enemy force or target accessible, other technologies will enhance the intelligence and precision of the weapons used to engage them.

Full Dimensional Protection

Full Dimensional Protection will be control of the battlespace to ensure our forces can maintain freedom of action during deployment, maneuver, and engagement while providing multilayered defenses for our forces and facilities at all levels. This concept has global implications for the joint force. To achieve a multilayered, seamless architecture of protection from the full array of enemy weaponry and electronic systems in both strategic and operational environments, all components of the joint force must evolve concepts and technologies which can be easily coordinated and synchronized.

Full Dimensional Protection

Concepts

Avoid Detection, Prevent Acquisition, Avert Hits, Survive Hits

Dispersed Operations

Early Warning and Counter Reconnaissance

Enhanced Limited Visibility Operations

Enablers

Improved Ballistic Protection

Multidimensional Joint Air and Missile Defense

Common Situational Awareness

Real-Time Intelligence with Vertical and Horizontal Distribution

Speed, Agility, Long-Range Weapons

Technologies

Advanced Soldier Technologies

Chemical and Biological Protection Ensembles

Reduced Signature Enhancements

Situational Understanding

Advanced Identification Technologies

The Army's approach to force protection will be a holistic one, applying organizational, materiel, and procedural solutions to the challenge of protecting soldiers, information, and equipment across the full spectrum of operating environments. It will complement the capabilities of the other components to assure the joint force freedom of strategic deployment, lodgment, expansion, and maneuver without surprise or significant disruption by any enemy force. These capabilities will include an array of fused sensors and area defenses to protect critical, high-value operational and strategic assets from enemy air, land, and sea attack.

To protect the force, the Army will rely on a technically advanced, operationally simple network of multicomponent intelligence sources capable of detecting and locating forces, active and passive obstacles, in-flight aircraft, ballistic and cruise missiles and their launch sites, chemical and biological agents, electronic jamming sources, and a host of still-developing threats. Missile system technologies, to defeat both air-to-surface and surface-to-surface systems, will be leveraged to enable successful engagements at ranges sufficient to provide multiple shot opportunities well before the defended areas are penetrated. Hit-to-kill technologies will neutralize chemical or biological warheads over enemy territory. Manned and unmanned platforms will contribute to the weave of sensor and weapon capabilities so that the reach of full dimensional protection can extend far beyond the horizon. Significantly more sensors will provide refined information to even more elements at lower echelons, enhancing total force situational understanding, enabling greater dispersion, and minimizing the risk of fratricide.

Advanced technologies will provide vastly improved personal armor, chemical and biological protection ensembles, and reduced signature enhancements. Many of those concepts and technologies developed to support dominant maneuver will also contribute to protecting the force.

Both at home and abroad, the Army will contribute to the strategic defense of the United States. Fitting into a detection and command and control architecture with the air and sea components, the Army will provide the teeth of the missile engagement capability, to protect the U.S. land mass against its most serious external threat—missile attack.

Focused Logistics

Focused logistics will be the fusion of information, logistics, and transportation technologies to provide rapid crisis response, to track and shift assets even while en route, and to deliver tailored logistics packages and sustainment directly at the strategic, operational, and tactical level of operations.

Focused Logistics

Concepts

Anticipatory Logistics and Personnel Support

Split-Based Operations

Sustained Tempo

Enhanced Throughput Operations

Velocity Management

Battlefield Distribution System

Total Asset Visibility

Objective Supply Capability

Enablers

Integrated Maneuver and Combat Service Support

Systems Command and Control

Total Asset Visibility

Modular Organization

Movement Tracking System

Wireless Management Information Systems

Technologies

Information Age Technologies for Inventory Control

More Durable Materials

Over-the-Air Software Diagnostics and Repair

Automated Cross-Leveling and Rerouting

For the Army, focused logistics will be the fusion of logistics and information technologies, flexible and agile combat service support organizations, and new doctrinal support concepts to provide rapid crisis response to deliver precisely tailored logistics packages directly to each level of military operations.

Technology, once again, will be a great enabler of the concept of focused logistics. Smaller fighting elements with easily maintainable equipment, made of more durable materials which share repair-part commonality among component-specific equipment and equipment in other components, will significantly reduce the volume and complexity of the resupply system. Precision weapons with increased lethality and survivability and fuel-efficient systems will generate reductions in demands on the sustainment infrastructure. Advanced business solutions for inventory control, materiel management and distribution, transportation and warehousing, and automatic cross-leveling and rerouting will greatly expand current Army Total Asset Visibility and Objective Supply Capability concepts. Semiautomatic, built-in diagnostic sensors will anticipate failure and initiate resupply or replacement activities before failures occur.

In the same way that built-in weapon system situational understanding software will be used to train combat crews, the situational understanding logistical network will enable suppliers to train, and will be used to “war game” operations so that supply analysts can develop alternatives and test logistics plans before operations occur. A vast array of advances in human support and medical care technologies, including “internet triage” and “telemedicine,” will greatly enhance the survivability of all members of the joint force.

Clearly, focused logistics is the most applicable operational concept across the patterns of operation. No other concept is executable without focused logistics, yet focused logistics is an operation which could stand alone, particularly in humanitarian missions. Inasmuch as the Army is organized and equipped to sustain itself in long-term, austere operational environments, it is especially suited to react quickly when called upon to provide logistic support for both domestic and foreign natural or man-made disasters.

Information Superiority

We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.

Information Superiority

Concepts

Seamless, Secure, Dynamic Communications

Continuous Real-Time IPB

Disrupt Enemy Information Operations

Protect and Conceal Friendly Information Operations

Installations as C4I Platforms

Enablers

Global Command and Control System (GCCS)

Construct, Connect, and Manage the Information Battlespace

Linked Strategic, Operational, and Tactical Sensors and C4I

"Smart-Jamming"

Sensor-Shooter Links

Technologies

Wireless Communications

Data Compression

Advanced Network Technology

Mobile, Very Small Satellite Transceivers

Multilevel Security Devices

Information operations (IO) conducted to gain information dominance are essential to all the patterns of operation. They consist of both offensive and defensive efforts to create a disparity between what we know about our battlespace and operations within it and what the enemy knows about his battlespace. Army IO is conducted within the context of joint IO, including PSYOPS and deception campaigns to ensure the strategic, theater, and tactical efforts are synchronized and collaborative.

In the aggregate, IO technologies will assist in understanding the battlespace. High-speed processors will fuse information from multiple sources while rapid generation of high-fidelity databases will enable the commander to visualize current and future operations. Bandwidth on demand will facilitate common understanding at all echelons and new antenna configurations will allow dissemination of “real time” information on the move. At the same time, low probability of intercept/low probability of detection signature management will protect friendly information while directed and RF energy will disrupt and deny information to the enemy.

Conclusion

In this unstable and turbulent world, the Army will continually be called upon to meet the Nation’s needs: from responding to hurricanes, forest fires, and other disasters; to internal security matters at Olympic and inaugural events; to humanitarian assistance; to shaping the future world environment through continuous contacts around the world; to peacekeeping; to nation building; and to conflict resolution. A versatile force is required to respond with little or no notice to this full spectrum of operations.

Army Vision 2010 foresees a capabilities-based Army with the proper mix of heavy, light, and Special Operations Forces (SOF) focused on the Euro-Middle East and Asian Arc regions of the world- a force trained, ready, and equipped to conduct full-spectrum operations, to do what needs to be done across the entire spectrum of crisis.

This versatile land force of the 21st century must retain the quality soldiers that comprise the Army today and recruit equally competent, motivated soldiers to replace them in the future to achieve a full-spectrum capability. Quality soldiers are essential to the successful execution of the operational concepts of *Joint Vision 2010* as well as *Army Vision 2010*.

America's Army is determined to meet the challenge. The Army in 2010 will be a Total Quality Force consisting of dedicated men and women, military and civilian, in both the active and reserve components. Along the way, we will team with private industry and the academic community at every opportunity as a means of assuring future vitality in the science and technology base, the industrial base, and the power projection base of our Army. The results of this eclectic effort will be a force of decision projected with lighter, more durable equipment to facilitate deployment and sustainability. In the theater of operations, information age technologies will facilitate shaping the battlespace to set the conditions for decisive operations, resulting in the successful accomplishment of all missions. From deployment through operations, transition to peace and redeployment, the force will be protected by technically advanced, operationally simple sensors, processors, and warfighting systems to ensure freedom of strategic and operational maneuver.

Most importantly, the concepts, enablers, and technologies addressed in *Army Vision 2010* will empower soldiers—not replace them. The Army of today is the product of 220 years of evolutionary change in doctrine, training, and leader development programs. The Army of tomorrow will be borne of that same process—grounded in the values, traditions, and heritage that are uniquely American. We are committed to forging that Army—to conduct prompt and sustained operations on land throughout the entire spectrum of crisis, AND to do what needs to be done as part of the joint warfighting team envisioned in *Joint Vision 2010*. Stability in the world is assured by the presence and influence of the United States Army—Yesterday, Today, and Tomorrow.

CHAPTER 8

GLOBAL ENGAGEMENT:

A VISION FOR THE 21ST CENTURY AIR FORCE

The Security Environment is Changing

Change in the world around us requires change in the Air Force. The end of the Cold War swept away national security requirements that had appeared to be fixtures of the global security landscape. The Air Force anticipated the change and produced a vision for dealing with the post-Cold War world in the ground-breaking document, *Global Reach—Global Power*. This vision has guided the restructuring and modernization of the Air Force for the past 6 years. Because the change and uncertainty of the immediate post-Cold War era will endure, the Air Force must forge a new vision that will guide it into the 21st century.

To enable the Air Force to meet the challenges of change, the Secretary and Chief of Staff of the Air Force initiated a rigorous, systematic, multi-faceted examination of future demands on the Air Force as a member of America's joint military force. This revolutionary effort has had the deep involvement of Air Force leaders. It was guided by a Board of Directors consisting of senior military and civilian leaders, and chaired by the Air Force Vice Chief of Staff.

After extensive study and discussion, the Air Force senior leadership began to build this Air Force vision for the 21st century. It was shaped by *Joint Vision 2010*, the new guidance published by the Chairman of the Joint Chiefs of Staff. Air Force leaders understood that their new strategic vision must meet the national security needs of the nation, and a national military strategy that has as its focus an increasingly U.S.-based contingency force. The Air Force also recognizes the emerging reality that in the 21st century it will be possible to find, fix or track and target anything that moves on the surface of the earth.

Global Engagement: A Vision for the 21st Century Air Force is based on a new understanding of what air and space power mean to the nation—the ability to hit an adversary's strategic centers of gravity directly as well as prevail at the operational and tactical levels of warfare. Global situational awareness, the ability to orchestrate military operations throughout a theater of operations and the ability to bring intense firepower to bear over global distances within hours to days, by its very existence, gives national leaders unprecedented leverage, and therefore advantages.

This strategic vision addresses the entire Air Force—people, capabilities and infrastructure—and charts the course of the Air Force into the first quarter of the 21st century. The vision is the first step in the Air Force's back-to-the-present approach to long-range planning. Although this strategic vision document establishes overall direction, the Air Force will develop a Long-Range Plan to make the vision come true. Formulating a coherent, shared strategic vision is a critical step, but the real challenge is to make the vision actionable and implementable.

Today's Air Force

Explorations of the future must proceed from where the Air Force stands today: the world's most powerful air and space force. New technology and new operational concepts already offer an alternative to the kind of military operation that pits large numbers of young Americans against an adversary in brute, force-on-force conflicts. This new way of war leverages technologically superior U.S. military capabilities to achieve national objectives. It is a strategy of asymmetric force that applies U.S. advantages to strike directly at an adversary's ability to wage war. It offers potentially decisive capabilities to the Joint Force Commander to dominate the conduct of an adversary's operations across the spectrum of conflict.

But technology and tactics only go so far. Our core values, history, mission and the professionalism with which they are brought together are what make us the institution we are today. Our core values are simple and forthright: Integrity first. Service before self. Excellence in all we do….Our challenge is to dominate air and space as a unique dimension of military power. Global Engagement provides the strategic blueprint for meeting that challenge.

Planning Into the Next Century

For all the transformation the world will undergo in the next 30 years, fundamental U.S. national security objectives will remain largely as they have been for the past 220 years: to ensure our survival as a nation, secure the lives and property of our citizens, and protect our vital national interests.

Securing those vital interests under future conditions, however, will significantly change the demand for U.S. military capabilities into the 21st century. In *Joint Vision 2010*, the Chairman of the Joint Chiefs of Staff has provided a common direction for our Services into the next century. The Chairman's vision calls for the capability to dominate an opponent across the range of military operations—Full Spectrum Dominance. The plan to achieve this goal comprises four operational concepts to guide future joint warfare development—Dominant Maneuver, Precision Engagement, Full-Dimensional Protection, and Focused Logistics. In addition, Full Spectrum Dominance requires Information Superiority, the capability to collect, process, analyze and disseminate information while denying an adversary's ability to do the same.

These concepts form a lens through which the Air Force looks to the first quarter of thc 21st century.

Air and Space Power for the Next Century

Full Spectrum Dominance depends on the inherent strengths of modern air and space power—speed, global range, stealth, flexibility, precision, lethality, global/theater situational awareness and strategic perspective. Air and space power also contributes to the level of engagement and presence necessary to protect and promote U.S. national interests by augmenting those forces that are permanently based overseas with temporary or rotational deployments and power projection missions.

Ensuring that air and space power continues to make its unique contributions to the nation's Joint Team will take the Air Force through a transition of enormous importance. We are now transitioning from an air force into an air and space force on an evolutionary path to a space and air force. The threats to Americans and American forces from the use of space by adversaries are rising while our dependence on space assets is also increasing. The medium of space is one which cannot be ceded to our nation's adversaries. The Air Force must plan to prevail in the use of space.

Space is already inextricably linked to military operations on land, sea and in the air. Several key military functions are migrating to space: Intelligence, Surveillance and Reconnaissance (ISR); warning; position location; weapons guidance; communications; and, environmental monitoring. Operations that now focus on air, land and sea will ultimately evolve into space.

All the Services depend heavily on space assets to support their missions. The Commander-in-Chief of U.S. Space Command (USCINCSPACE) is already tasked with the missions of space control and force application in support of the joint warfighter. The Air Force will sustain its stewardship of space and will fully integrate Air Force space capabilities in joint efforts to support the needs of the nation.

The Air Force recognizes that any further use of space will be driven by national policy, international events, threats moving through and from space, and threats to U.S. space assets. However, the nation will expect the Air Force to be prepared to defend U.S. interests in space when necessary.

Core Competencies

Our core competencies represent the combination of professional knowledge, airpower expertise, and technological know-how that, when applied, produces superior military capabilities. A particular core competency is not necessarily unique to the Air Force. Speed, flexibility, and the global nature of its reach and perspective distinguish the Air Force's execution of its core competencies.

The first quarter of the 21st century will demand that the Joint Force Commander field robust, flexible capabilities to cope with a wide range of contingencies. Each military service must present to the combatant commander a set of relevant and complementary capabilities. This presentation allows the Joint Force Commander to consider all options available, and to tailor campaign plans to best meet the military objectives of the mission.

The Air Force contribution to the Joint Force Team…begins with a foundation of quality people. Air Force men and women carry out the core competencies of Air and Space Superiority, Global Attack, Rapid Global Mobility, Precision Engagement, Information Superiority, and Agile Combat Support. These are…all mutually supporting and provide synergistic effects. These competencies are brought together by global awareness and command and control to provide air and space power to the Joint Force Team.

Within the Air Force, core competencies provide a bridge between doctrine and the acquisition and programming process. In the context of long-range planning, defining future core competencies provides strategic focus for the vision. Each core competency illuminates part of the strategic vision that will guide decisions and set the course toward the Air Force of the 21st century….

The key to ensuring today’s Air Force core competencies will meet the challenge of tomorrow is innovation. Innovation is part of our heritage as airmen. The Air Force was born of a new technology—manned powered flight. Innovation will enable the Air Force to evolve from an air force to an air and space force on its path toward space.

The Air Force is committed to a vigorous program of experimenting, testing, exercising and evaluating new operational concepts and systems for air and space power. It will provide additional emphasis in six areas of ongoing activity in Air Force centers of excellence. That will be accomplished with a series of focused battle laboratories for space, air expeditionary forces, battle management, force protection, information warfare, and unmanned aerial vehicles….

Core Competency: Rapid Global Mobility

Rapid Global Mobility provides the nation its global reach and underpins its role as a global power. The ability to move rapidly to any spot on the globe ensures that tomorrow, just as today, the nation can respond quickly and decisively to unexpected challenges to its interests.

As the number of forward-deployed forces declines and the need for immediate response to overseas events rises, the Air Force’s global mobility forces will be in great demand by future Joint Force Commanders. When an operation must be carried out quickly, airlift and aerial refueling will be the key players. Rapid Global Mobility may build an air-bridge for joint forces, enable multi-national peace efforts, or speed tailored support to forces already on the scene.

Rapid deployment will remain the future Joint Team's most reliable combat force multiplier. Fighter forces paired with precision weapons provide formidable capabilities that our mobility fleet can deploy worldwide and sustain at high in-theater sortie rates. In other cases, such as delivery of humanitarian relief, the rapid delivery of material is the focus of effort.

In the 21st century, Rapid Global Mobility will be multi-faceted. Better use of commercial carriers will be made to increase the efficiency of Air Force mobility. The speed with which forces are moved will increase, and airlift and air refueling capabilities must be able to deliver tailored forces operating with a smaller footprint.

Core Competency: Precision Engagement

Joint Vision 2010 defines Precision Engagement as the capability "that enables our forces to locate the objective or target, provide responsive command and control, generate the desired effect, assess our level of success, and retain the flexibility to re-engage with precision when required." The Air Force's core competency of Precision Engagement is grounded in the Joint definition. Its essence lies in the ability to apply selective force against specific targets and achieve discrete and discriminant effects. The nation needs the precise application of military capability to meet policy objectives. The Air Force's Precision Engagement core competency provides the nation with reliable precision, an ability to deliver what is needed for the desired effect, but with minimal risk and collateral damage.

Technology has driven each military era's definition of precision. In the 21st century, it will be possible to find, fix or track, and target anything that moves on the surface of the earth. This emerging reality will change the conduct of warfare and the role of air and space power. As Air Force members, we have a responsibility to understand, develop and advocate new ways that air and space power can serve the nation and the Joint Force Commander. We must develop new operational concepts that clearly address how air and space power can achieve directly or contribute to achieving the full range of joint campaign objectives. Our ideas and doctrine must be as creative and flexible as the instrument itself.

When conflict occurs, the Air Force of the 21st century must be able to offer options for the employment of force in measured but effective doses. To do so, the Air Force will rely on global awareness capabilities to support national decision-making and joint operations to determine military objectives and enable precise targeting. Air and space forces will then apply power that is no less overwhelming because it is also discriminating. Discriminating effects are selective; they aim for efficiency and steer away from unwanted collateral damage. The Air Force core competency of Precision Engagement will remain a top priority in the 21st century.

Core Competency: Global Attack

The ability of the Air Force to attack rapidly anywhere on the globe at any time is unique. The military utility of air power, particularly its speed, range, and flexibility prompted creation of the Air Force as a separate Service following World War II. With the advent of the

Cold War, Air Force long-range bombers and later intercontinental ballistic missiles began their vital roles in the nation's first priority of deterring nuclear war. Although nuclear weapons no longer play as central a role in America's national security strategy as they did during the Cold War, we recognize the dangers posed by the efforts of rogue states and others to acquire them. The Air Force will sustain its efforts in the nuclear area and strengthen its response to the growing risk of proliferation. To this end, the Air Force will maintain the bomber and land-based ballistic missile legs of the Triad while remaining prepared to undertake further reductions as circumstances require. The Air Force will also sustain its commitment to support the nuclear requirements of the theater CINCs. Moreover, the Air Force remains absolutely determined to maintain its record of excellence as the custodian of nuclear weapons by ensuring the safe and secure operation of those weapons.

Air Force short- and long-range attack capabilities continue to support the deterrence of conventional warfare by providing versatile, responsive combat power able to intervene decisively when necessary. The ability of the Air Force to engage globally, using both lethal and non-lethal means, is vital to today's national security strategy of Engagement and Enlargement. At present, almost a quarter of Air Force personnel are deployed overseas at any one time. The Air Force will maintain that level of commitment and will employ air and space power aggressively to meet the nation's needs for presence and power projection. Over time, however, technological change, threats to forward bases, asymmetric strategies by adversaries who seek to deny entry to U.S. power projection forces, and growing budgetary pressures will likely change the way the Air Force carries out its presence and power projection missions.

The Air Force has developed and demonstrated the concept of an Air Expeditionary Force (AEF) rapidly deployable from the United States. This expeditionary force can be tailored to meet the needs of the Joint Force Commander, both for lethal and non-lethal applications, and can launch and be ready to fight in less than 3 days. The Air Force will develop new ways of doing mobility, force deployment, protection, and sustainability in support of the expeditionary concept.

Air Force power projection and presence capabilities today are a complementary mix of long-range and theater aircraft, based in the United States and forward-based. The Air Force has relied heavily in the past on the elements of that mix that were permanently forward-based overseas. Currently, the Air Force is increasing the role of expeditionary forces to maintain its global engagement capability. In the future, capabilities based in the continental United States will likely become the primary means for crisis response and power projection as long-range air and space-based assets increasingly fill the requirements of the Global Attack core competency.

Core Competency: Air and Space Superiority

Superiority in air and space—control over what moves through air and space—delivers a fundamental benefit to the Joint Force. It prevents adversaries from interfering with operations of air, space or surface forces, and assures freedom of action and movement. The control of air and space is a critical enabler for the Joint

Force because it allows all U.S. forces freedom from attack and freedom to attack. With Air and Space Superiority, the Joint Force can dominate enemy operations in all dimensions—land, sea, air and space.

Gaining Air and Space Superiority is not just operationally important. It is also a strategic imperative for protecting American lives throughout a crisis or conflict. It is the precursor for Dominant Maneuver and is also the basis of Full-Dimensional Protection. Strategic attack and interdiction—crucial to the outcome of any battle—are not possible without air superiority. Effective surface maneuver is impossible without it. So is efficient logistics. The bottom line is everything on the battlefield is at risk without Air and Space Superiority. Moreover, if air dominance is achieved and joint forces can operate with impunity throughout the adversary's battlespace, the Joint Force Commander will prevail quickly, efficiently, and decisively.

Defense against ballistic and cruise missiles is an increasingly important element of Air and Space Superiority. The rapidly growing theater and global threat posed to Americans and America's interests by cruise and ballistic missiles is one of the developments which is accelerating warfare along the air-space continuum. The Air Force is moving aggressively to counter this threat. Although the global and theater missile threats are now addressed separately, over time they will merge into a common missile defense architecture, becoming a single counter air and space missile defense mission.

Core Competency: Information Superiority

In no other area is the pace and extent of technological change as great as in the realm of information. The volume of information in joint warfare is already growing rapidly. The ability of the future Joint Team to achieve dominant battlefield awareness will depend heavily on the ability of the Air Force's air- and space-based assets to provide global awareness, intelligence, communications, weather and navigation support. While Information Superiority is not the Air Force's sole domain, it is, and will remain, an Air Force core competency. The strategic perspective and the flexibility gained from operating in the air-space continuum make airmen uniquely suited for information operations.

Providing Full Spectrum Dominance requires a truly interactive common battlespace picture. The Air Force is committed to providing the integrated global and theater air, space and surface picture of the battlespace to the 21st century Joint Force Commander. Moreover, its future Battle Management/ Command and Control (BM/C2) systems will enable real-time control and execution of all air and space missions. The Air Force will also ensure that its information systems will be fully interoperable for seamless integrated battlespace management.

The Air Force will exploit the technological promise of Unmanned Aerial Vehicles (UAVs) and explore their potential uses over the full range of combat missions. The highest payoff applications in the near-term are Intelligence, Surveillance, Reconnaissance (ISR) and communications. A dedicated Air Force UAV squadron will focus on operating the Predator medium-range surveillance UAV, which also will serve as a testbed for developing concepts for operating high altitude, long endurance UAVs. In the mid-term, the Air Force expects that suppression-of-enemy-air defense (SEAD) missions may be conducted from UAVs, while the migration of additional missions to UAVs will depend upon technology maturation, affordability and the evolution to other forms of warfare.

Information Operations, and Information Warfare (IW) in particular, will grow in importance during the 21st century. The Air Force will aggressively expand its efforts in defensive IW as it continues to develop its offensive IW capabilities. The top IW priority is to defend our own increasingly information-intensive capabilities. Already dedicated and operational in the garrison defense of computer systems, the Air Force will continue to invest in defensive IW, and move to defend its forward-deployed assets, particularly in BM/C2. On the offensive side, the Air Force will emphasize operational and tactical IW and continue, in conjunction with other Federal agencies, to support strategic information operations.

Core Competency: Agile Combat Support

Agile Combat Support is recognized as a core competency for its central role in enabling air and space power to contribute to the objectives of a Joint Force Commander. Effective combat support operations allow combat commanders to improve the responsiveness, deployability, and sustainability of their forces. The efficiency and flexibility of Agile Combat Support will substitute responsiveness for massive deployed inventories.

Combat operations in the 21st century will require highly responsive and agile forces. The Air Force leadership adopted the concept of time-definite resupply, a fundamental shift in the way we support deployed forces. Resupply of deployed forces will begin upon arrival, reducing their initial lift requirement. Time-definite delivery will form the basis for all resupply in the theater, thus reducing total lift requirement. When combat commanders require an item, the system will reach back to the continental United States and deliver it where and when it is needed. This reach-back approach will make it possible to deploy fewer functions and personnel forward for the deployment and sustainment processes. This, in turn, will reduce the size and therefore the vulnerability of our forces forward. Providing for force protection is not just a matter of airbase operability and security, as important as they are. It also involves the redesign of our power projection forces to reduce the size of the force protection problem.

To provide Agile Combat Support, information technology must be leveraged to improve command and control which is key to accurate and timely decisions. As an example, the ability to know the location of critical parts, no matter which Service or agency holds the parts, will allow enormous gains in efficiency. The Air Force depot system will continue to reduce cycle times and streamline its infrastructure. Outsourcing and privatization, as well as other Services' capabilities, will be major tools in helping to move the materiel required for deployed forces from "factory to flightline." These concepts will be pursued, first in the context of the Air Expeditionary Force and, once matured, for the 21st century force.

Agile Combat Support's essential contribution to air and space combat capability complements the Joint designation of Focused Logistics as an operational concept, which is indispensable to achieving Full Spectrum Dominance.

Air Force People

People are at the heart of the Air Force's military capability, and people will continue to be the most important element of the Air Force's success in capitalizing on change. The Air Force of tomorrow and beyond must encourage individuals to be comfortable with uncertainty and willing to make decisions with less than perfect information. Accordingly, our people must understand the doctrine, culture, and competencies of the Air Force as a whole—in addition to mastering their own specialties. Emphasis on creating an Air Force environment that fosters responsiveness and innovation, and rewards adaptability and agility will be crucial as we move into the early part of the next century. Many things may change, but the Air Force of the first quarter of the 21st century will continue to place a high priority on maintaining the high quality of its men and women, and on providing quality of life for Air Force members and their families.

The Total Force of the Future

One sign of change in the Air Force will be how the definition of the Air Force operator develops in the future. At its birth, all Air Force operators wore wings. Future definitions of operators will change as the Air Force changes. Moreover, all combat operations in the 21st century will depend on real-time control and employment of information, further broadening the definition of the future operator. In the future, any military or civilian member who is experienced in the employment and doctrine of air and space power will be considered an operator.

The composition of the future Total Force will change as the nature of air and space power changes. As a result, the Air Force is committed to outsourcing and privatizing many functions now performed internally. The force will be smaller. Non-operational support functions will increasingly be performed by Air Force civilians or contractors. Most uniformed personnel will be operators and a greater percentage will be from the Reserve components.

To prepare for the changes ahead, the Air Force has reviewed, generally reaffirmed, and initiated some adjustments to its career development patterns for its officers, enlisted, and civilian force. To ensure its future leaders all share a full and common understanding of air and space operations, the Air Force decided to create a new Air and Space Basic Course. This course will focus on the history, doctrine, strategy, and operational aspects of air and space power. The desired outcome is for each new officer and selected senior NCOs and civilians to have a thorough knowledge of the day-to-day capabilities of combined air and space operations. Most officer graduates from this course will go directly to operational jobs as their first assignment before performing their functional specialty.

The Air Force will seek new opportunities to capitalize on the synergy of the Air National Guard and Air Force Reserve forces in an integrated TOTAL Force. In its effort to maximize and improve operational effectiveness and efficiency, the Air Force will explore additional opportunities for new Guard and Reserve missions as well as expanding the use of Individual Mobilization Augmentees (IMAs). The Air Force's ability to rely upon and integrate its Reserve components is already a fundamental strength, one that will continue to play a major role for the nation in the next century.

A Force Grounded in Core Values

The ideals embodied in the Air Force core values are: Integrity first. Service before self. Excellence in all we do.

They are universally prescriptive. Despite the uncertainty of the future, the Air Force can say with certainty that today and tomorrow, it must live up to these ideals or it cannot live up to its responsibilities. Our core values are fundamental and timeless in nature, and reach across the entire force. Our core values are values for service, values for life, and must be reflected in everything that we do.

A values-based Air Force is characterized by cohesive units, manned with people who exhibit loyalty, who want to belong, and who act in a manner consistent with Air Force core values, even under conditions of high stress. To ensure this values-based Air Force, three elements—education, leadership and accountability—provide a framework to establish the strongest imprint of shared Air Force core values. In the Air Force of tomorrow, as in the Air Force of today, these stated and practiced values must be identical.

The Air Force will continue to reinforce its core values in all aspects of its education and training. The goal is to provide one hundred percent of the Total Force with core values education and training continually throughout a career. The Air and Space Basic Course will also ensure that the Air Force's future leaders, military and civilian, have a common, shared foundation in core values, doctrine, and operations.

Key Elements of Air Force Infrastructure

Defining our future core competencies tells us what business the Air Force will be in as it enters the 21st century. But the Air Force must change the way it does business if it is to meet the future demands for air and space power. Continuing pressure on resources will make increased efficiency and reduced infrastructure costs necessary for success.

The Air Force has long recognized the importance of responsible stewardship of taxpayer dollars and will strive to achieve the highest standards for efficiency. Ensuring the nation has capabilities to hedge against unforeseen and multiple threats across the full spectrum of conflict puts a premium on efficiency. The real penalty for inefficiency is not just wasted dollars, but unmet demand for military capabilities.

Our warfighting activities will be designed for effectiveness and our support activities will be designed for efficiency. All support activities will be run more like businesses, using the "best practices" gleaned from top performers. Air Force personnel will focus on preparing for and conducting military operations—their competence—while support activities not deployed for combat will be performed by a robust civilian and competitive private sector. The

Air Force is committed to the organizational and cultural change to make this vision a reality.

The Air Force will increase the efficiency of its modernization process through the focused exploitation of emerging information technologies and by accelerating its ongoing acquisition reform program. It also will strengthen the concept of integrated weapon system management by clarifying relationships between single-product managers, their customers and the depot and contracted activities that support them.

The Air Force is committed to the aggressive reduction of infrastructure costs. The role of commercial industry will be maximized to ensure "best-value practices" throughout the development and production process. These activities—research, development, testing and evaluation (RDT&E), and sustainment—will be consolidated into Centers of Excellence encompassing mission areas directly related to Air Force core competencies. The Air Force will also explore teaming with the other services to form Joint Centers of Excellence for RDT&E.

Inefficiency drains resources needed for the capabilities the nation needs from its future joint force team. The overlap and redundancy of test and evaluation facilities must be reduced through streamlining, integration, outsourcing, and privatization. New technologies, particularly in testing through modeling and simulation, must be exploited to reduce costs and improve effectiveness.

The Air Force's determination to become more efficient will also affect the composition of its future workforce. Its commitment to an aggressive program of civilianizing many combat support functions, as well as outsourcing and privatization, will push more support functions into the civilian workforce and, in many cases, into the private sector.

The Air Force believes that one of its most important attributes is a sense of community among its members and their families. Far more than simple “pride in the team,” this factor builds the motivational identity and commitment that underlie our core values, career decisions, and combat capability. The excellence of our installations and Quality of Life standards contribute to this, and to the general well-being of the members of the Air Force family. The Air Force is rededicating itself to both maintaining this sense of community and finding new and more efficient ways of providing it.

Looking Back to the Present to Plan for a New Century

This document sets out a new Air Force strategic vision for the 21st century. It provides a vision of the future and a path back to the present to guide today’s planners. Following this path requires a revitalized and institutionalized long-range planning process.

The Long-Range Plan will identify those initial steps and transition decisions which are necessary to reach the goals outlined in this strategic vision document. Transition decisions are critical to formulating meaningful divestment and investment strategies, to making transitions from sunset to sunrise systems and capabilities, and to providing the milestones and feedback mechanisms that ensure accountability. The Long-Range Plan will further guide the Air Force’s other planning and resource allocation processes.

Final Thoughts

Global Reach—Global Power prepared the Air Force to deal with the challenges of the transition era following the Cold War. *Global Engagement: A Vision for the 21st Century Air Force* charts a course that will take the Service beyond this transitional period and into the future. It is a future in which dramatic changes wrought by technology will be the norm. It is also a future in which the core values of service, integrity, and excellence will continue to sustain the men and women of the Air Force. Most importantly, the Air Force's devotion to air and space power will continue to provide the strategic perspective and rapid response the nation will demand as it enters the 21st century.

Our Vision Statement remains: Air Force people building the world's most respected air and space force…global power and reach for America.

CHAPTER 9

FORWARD...FROM THE SEA

Introduction

The Navy's unique contributions to national security stem from the advantages of operating on, under, above, and from the sea. This is the message of *Forward…From the Sea*. The primary purpose of forward-deployed naval forces is to project American power from the sea to influence events ashore in the littoral regions of the world across the operational spectrum of peace, crisis, and war. That is what we do. This paper describes how we do it today, and how we will do it in the future.

The roles of America's armed forces are defined by the three components of the National Military Strategy: peacetime engagement, deterrence and conflict prevention, and fight and win. Although national policy changes as the strategic landscape evolves, there will be continued emphasis on using the armed forces across this spectrum. Operations in peacetime and crisis to maintain regional economic and political stability are traditional roles of the Navy-Marine Corps team. These roles are rooted in our fundamental ability to maneuver independently of political constraints and fight and win. A key operational advantage of forward-deployed naval forces is that we provide on-scene capabilities for executing simultaneously all three components of the National Military Strategy, and do so without infringing on any nation's sovereignty. This advantage exists because we operate in international waters. Our hallmark is forward-deployed forces with the highest possible readiness and capability to transition instantly from peace to crisis to conflict. This flexibility positions us to fight and win early, or to contain conflict. More importantly, our presence may prevent conflict altogether. By any standard or measure, peace is cheaper than war.

Our forces are optimized for this forward role in national strategy. As we enter the 21st century, we will continue to develop and adopt innovative concepts and technologies to remain the force on the cutting edge of our nation's defense.

How the Navy Operates

Forward…From the Sea provides the basis for a simple, yet powerful, operational concept of how we will operate to carry out expeditionary operations. We conduct forward naval operations both to ensure unimpeded use of the seas and to project American influence and power into the littoral areas of the world. Expeditionary operations achieve U.S. objectives across the spectrum of the National Military Strategy. They are a potent and cost-effective alternative to power projection from the continental United States and are suited ideally for the many contingencies that can be deterred or quickly handled by forward-deployed forces. Expeditionary operations complement, enable, and dramatically enhance the effectiveness of continental power-projection forces when a larger military response is needed.

Our attention and efforts will continue to be focused on operating in and from the littorals. The landward side of the littoral can be supported and defended directly from the sea. It encompasses areas of strategic importance to the United States. Seventy-five percent of the Earth’s population and a similar proportion of national capitals and major commercial centers lie in the littorals. These are the places where American influence and power have the greatest impact and are needed most often. For forward-deployed naval forces, the littorals are a starting point as well as a destination. Tactically, the distance we reach inland from the sea depends on terrain and weather, the contributions of joint and coalition forces, the potential adversary’s capabilities, and the nature of our mission. The mission may require us to exercise our considerable reach and operate far inland.

We will deploy carrier battle groups and amphibious ready groups with embarked Marines to provide naval expeditionary forces for the Combatant Commanders. When required, we deploy separate units—such as for maritime interception force operations—but each remains capable of being integrated into a larger naval expeditionary force. We train carrier battle groups and amphibious ready groups together to ensure immediate readiness for a wide range of contingencies. Once overseas, we disperse the force and maintain a dynamic presence posture. Our forces are constantly in motion to make their capabilities visible throughout the theater while carrying out numerous simultaneous missions in support of U.S. interests. We can operate individual units—such as submarines—independently or completely integral to the force. We link dispersed units as an integrated force with command and control networks. When necessary for a specific crisis-response operation, we rapidly assemble elements of the force into a mission-tailored task group, such as a surface battle group. We rapidly converge from our forward deployment hubs to the scene of a potential conflict to deter aggression or to project power should deterrence fail. We take advantage of the reach of our sensors and weapons to project power over vast areas from a dispersed, networked force—concentrating combat power rather than our platforms and delivering firepower far inland when required by the mission. We are on-scene and ready for peacetime engagement, deterrence and conflict prevention, and fighting and winning.

Peacetime Engagement

The Navy's role in peacetime engagement is to project American influence and power abroad in support of U.S. efforts to shape the security environment in ways that promote regional economic and political stability. Stability fosters a sense of security in which national economies, free trade practices, and democracies can flourish. Democratic states, especially those with growing economies and strong trade ties, are less likely to threaten our interests and more likely to cooperate with the United States. This stability and cooperation, which our peacetime engagement promotes, assists in meeting security threats and promoting free trade and sustainable development. We execute peacetime engagement by staying constantly engaged abroad as a visible tool of U.S. foreign policy and by supporting U.S. coalition-building efforts.

Naval forces are constantly engaged abroad in peacetime as a visible tool of U.S. foreign policy. Our global presence ensures freedom of navigation on international trade routes and supports U.S. efforts to bring excessive maritime claims into compliance with the international law of the sea. When disaster strikes, we provide humanitarian assistance, showing American compassion in action. Our forward deployments always include a wide range of diplomatic activities, such as: sending Sailors and Marines ashore as representatives of the American people; bringing foreign visitors onto sovereign U.S. naval vessels; and carrying out a wide range of community relations activities. These efforts promote American democratic ideals abroad, enhance mutual respect and understanding with the peoples of other countries, and demonstrate U.S. support for friendly governments. Our forces support U.S. diplomatic efforts aimed at shaping the security environment, such as improving relations with former adversaries or reducing tensions with potential adversaries. We take advantage of our mobility and sovereignty at sea to extend the reach of U.S. peacetime engagement efforts to countries not readily accessible by other forces.

Our forward-deployed forces support peacetime coalition building efforts. We exercise and train frequently with the naval, ground and air forces of friendly nations, improving our ability to operate together and increasing mutual understanding, confidence, and respect. These exercises allow us to explore means of coordinating the operations of diverse forces to achieve maximum combat power. We build confidence in U.S. security pledges by demonstrating our ability to ensure that land-based forces deploying from the continental United States will have ready access to the region in a crisis.

Deterrence and Conflict Prevention

Signaling with military forces is an important element of deterring aggression and preventing conflicts, and forward-deployed naval forces are a superb means of signaling U.S. capabilities and resolve to friend and foe alike. Credible military presence in areas of long-standing interest or immediate concern reaffirms the U.S. leadership role abroad, reassures allies with tangible proof of U.S. commitment to their security, and helps prevent potential sources of instability from generating crises. We deter by putting potent combat power where it cannot be ignored, and by serving as a highly visible symbol of the overwhelming force the United States can deploy to defeat aggression. We enhance the credibility of conventional deterrence by demonstrating our combat capabilities in live-fire training and in exercises with friends and allies.

In peacetime, we position the wide range of capabilities inherent in naval expeditionary forces where they are readily available for any contingency. Operating in international waters, our forces are sovereign extensions of our nation, free of the political constraints that can hamper land-based forces. We put the right capability in the right place at the right time. We possess the unique capability of responding to ambiguous warning that either would not justify costly deployments from the continental United States, or might be insufficient to persuade nations in the region to host U.S. forces on their soil. When a visible presence might be provocative or foreclose U.S.

military options, we can position submarines covertly to provide on-scene surveillance capabilities and firepower. Rotational deployments allow us to maintain our forward posture indefinitely. We spread our surveillance and reconnaissance capabilities across a wide area, providing detailed coverage that improves our knowledge and understanding of the region. We maintain combat readiness during forward operations by training and exercising regularly for potential contingencies. As we carry out peacetime tasks in distant waters, we often are laying the groundwork for a crisis-response operation or joint campaign that has not yet even begun.

Ballistic missile submarine (SSBN) deterrence patrols will continue to be an essential element of U.S. strategy for deterring a wide range of potential threats. SSBNs are central to U.S. nuclear strategy due to their stealth and survivability, the reliability and security of their command and control systems, and the accuracy and flexibility of their weapons.

Forward-deployed naval forces rapidly bring a wide range of capabilities to bear in crisis response operations. We can take direct action to protect American lives and interests, to prevent an unstable situation from deteriorating further, and to control or even resolve a crisis. In recent years, naval crisis response has included landing Marines to reinforce endangered U.S. embassies, non-combatant evacuation operations, maritime interception operations to enforce international sanctions, show of force operations to counter intimidation and deter aggression, escort operations to protect shipping endangered by a local conflict, and air and missile strikes against transgressors. We provide on-scene command and control capabilities for rapidly executing joint crisis response operations. Our self-sustaining endurance allows us to remain on scene as long as necessary to stabilize or resolve the situation. When required, we rapidly redeploy—without incurring additional expense or political debts—to deter a potential aggressor who might exploit U.S. involvement in a major contingency elsewhere.

Naval deterrence and crisis-response operations prevent aggressors from achieving a fait accompli. Having combat-credible naval forces on scene shapes the battlespace and demonstrates our capability to halt aggression early in a conflict, well before the aggressor can achieve his objectives. These efforts to deter aggression and resolve crises, while prudent, do not always succeed—but our efforts make a profound difference in how we think about our role in a potential conflict. Our ability to shape the battlespace well before a joint campaign commences is vital because even small changes in the early stages of a conflict can have a major impact on its outcome. We focus on halting aggression early in a conflict. We enhance the credibility of deterrence by thwarting the potential aggressor who hopes to prevail by delaying or disrupting the U.S. response.

Our organic intelligence, surveillance, and reconnaissance capabilities augment national sensors, enhancing U.S. awareness of a potential aggressor’s activities. We can do this overtly—with surface ships and aircraft—signaling U.S. interest in the situation and covertly—with submarines and Naval Special Warfare units—learning what we need to know without being provocative or tipping our hand as to our future intentions.

On-scene naval forces begin shifting the strategic and operational situation in the favor of the U.S. and its allies by forcing a potential aggressor to consider our combat capability when formulating his plans. We make it exceedingly difficult for an adversary to target us and deny him the option of pre-emption by keeping our forces dispersed and moving, by operating unpredictably or covertly, and by employing deception. The wide range of options we provide for immediate response to aggression leaves a potential aggressor uncertain of the intended U.S. course of action. This uncertainty keeps him off balance, disrupting his ability to formulate a coherent campaign plan and eroding confidence in his ability to effectively execute operation plans. Uncertainty may compel a leader to redeploy forces from his main objective to hedge against our wide range of capabilities. Our sensors can monitor such redeployments to detect weaknesses or gaps we can exploit. U.S. Navy and Marine Corps operations in the Arabian Gulf during Desert Shield demonstrated these advantages by pinning down significant Iraqi forces on Kuwaiti beaches during Desert Storm.

We extend our protective shield over allies, potential coalition partners, and critical infrastructure ashore to enhance the effectiveness of deterrence. Our emerging theater air and missile defense capabilities are particularly important elements of our shield. We create a sanctuary that neutralizes a potential aggressor's attempts at intimidation and encourages the perception that he is powerless to prevent the U.S. from reinforcing our allies. This reality may cause him to alter campaign plans, forego use of certain forces or weapons, or focus efforts on more limited objectives.

Fight and Win

We will take advantage of our robust command and control systems and the reach of our sensors and weapons to concentrate combat power from dispersed, networked forces and project power far inland. In contingencies of limited size and duration, we project power with decisive impact ashore. In larger conflicts, we are an integral part of joint operations to fight and win. We have a vital role throughout a joint campaign, from beginning to end.

Forward-deployed naval forces have a vital role in halting aggression early in a conflict. The United States normally enters a conflict in response to aggression against an ally or vital American interest. Consequently, U.S. and allied forces are usually on the strategic defensive early in a conflict. Our ability to deliver a wide range of naval firepower and generate very high aircraft sortie rates can have major impact on the course and outcome of a conflict, especially during this critical early period of a joint campaign, when continental U.S.-based forces are just starting to arrive in theater. We can use submarines, lurking covertly in littoral waters, to deliver naval fires or special operations forces where the enemy least expects to be attacked. Our forces also take offensive action to hold enemy centers of gravity at risk and seize the strategic advantage. We degrade and destroy enemy defensive systems with uniquely naval offensive operations, including suppression of enemy air defenses, leaving opponents vulnerable to sustained attacks. While we are crippling enemy defenses, we hit his offensive forces hard to disrupt important campaign objectives and to achieve a quick fait accompli.

Initial operations by forward naval forces are critical for enabling the joint campaign. We ensure access to the theater for forces surging from the United States by supporting coalition forces to keep them in the fight, by seizing or defending shore bases for land-based forces, and by extending our defensive systems over early-arriving U.S. joint forces ashore. Our ability to dominate the littorals, including the undersea environment, allows us to operate with impunity in the face of enemy area denial threats while taking initial action to defeat those threats and prepare the battlespace for follow-on forces. By defeating enemy area denial threats and keeping vital sea and air lanes open, we ensure an uninterrupted flow of reinforcements into the theater. We provide highly capable afloat command and control capabilities to launch initial combat operations without delay. For example, we lead early efforts to gain air superiority and take the war to the enemy by initially taking charge of the joint air battle as afloat Joint Force Air Component Commander. Our forward-deployed fleet flagships and carriers can provide fully equipped afloat command centers for the Commander Joint Task Force, as we did when USS MOUNT WHITNEY served as afloat JTF headquarters in Operation Restore/ Uphold Democracy in Haiti. Our afloat systems allow joint forces deploying from the continental United States to “plug” into on-scene networked command and control systems.

Our counter to the aggressor seeking to prevent the United States from bringing in overwhelming forces is to disrupt and exploit enemy efforts to target U.S. and allied forces. Area denial threats to joint air, ground, and maritime forces include enemy tactical and theater ballistic missiles, weapons of mass destruction, air threats, and sea denial capabilities. They also include enemy use of ground or special operations forces to seize or destroy vital en route and on-scene infrastructure ashore. Area denial threats are becoming more lethal, increasing U.S. force vulnerability. These threats cannot defeat us, but they can delay our response, prolong the conflict and increase the cost of thwarting aggression. Our ability to counter enemy area-denial threats effectively with potent information warfare, power projection and force-protection capabilities increases our decisive impact early in a joint campaign. The more an enemy depends on denial capabilities to achieve his objectives, the greater our impact when we defeat those capabilities.

Naval operations continue throughout the joint campaign. Naval operations include delivering precision naval fire, conducting naval operational maneuver, providing protection for joint and coalition forces ashore, keeping the seaborne logistics pipeline flowing, and remaining on scene after the joint campaign to enforce sanctions and maintain regional stability.

We deliver precision naval fires to accomplish strategic, operational, and tactical objectives. Precision means having the desired effect on the enemy, limiting collateral damage, lessening the risk to our forces, and achieving maximum impact with our combat resources. We can deliver all naval fires—strike, interdiction, and fire support—with the degree of accuracy required to accomplish the mission. We exploit the tactical depth we gain from our weapons reach to attack the enemy throughout the battlespace. Precision includes smart targeting, so that our ordnance is directed against key targets for greatest impact, and rapid, accurate battle damage assessment. New systems, such as unmanned aerial vehicles and afloat mission planning systems, are essential elements of smart targeting. Precision also includes extremely accurate delivery of “level-of-effort” munitions. We must organize our forces and focus their efforts to rapidly and decisively accomplish campaign objectives. Precision encompasses how we employ Naval Special Warfare forces and Marines, as well as naval fires. In some tactical situations, such as operations on urban terrain, a SEAL or Marine with a sniper rifle may be the optimum precision weapon.

The closely related concepts of naval operational maneuver and speed of command define how we employ naval combat power to have decisive impact ashore. Naval operational maneuver means using the advantages we gain by operating on and from the sea to establish operational and strategic advantage over enemy forces ashore. We do this by defeating enemy sea denial efforts and gaining maritime superiority, thus providing unimpeded use of strategic sea lanes and freedom of operation in littoral waters. We take advantage of our maritime superiority by operating in the fluid manner described earlier—dispersed, yet rapidly concentrated; constantly moving and ever changing; appearing to be a distant threat far over the horizon, then suddenly striking the enemy where he felt secure. Our simultaneous ability to attack the enemy throughout the battlespace with precision naval fires and Marine combat power generates an inescapable tactical quandary. Not knowing when or where we will strike, the enemy must either concentrate his forces where he guesses we will attack, or spread his forces to defend as many potential targets as possible. In either case, the enemy exposes weaknesses we can exploit.

Our superior speed of command enhances the advantages of operating from the sea. Speed of command is the ability to rapidly collect information, assess the situation, develop a course of action, and immediately execute with overwhelming effect. Just as in the modern high-tech market place, speed of command achieves disproportionately larger returns for relatively modest, but precisely placed, initial investments. This capability is characterized by extraordinarily high rates of change that lock out enemy solutions, while locking in our success. We use speed, deception, and surprise to create and exploit enemy vulnerabilities, to seize rapidly fleeting opportunities, and to shift the tactical and operational situation to our advantage. We apply combat power in a high-tempo continuum, vice in incremental steps, to keep the enemy disoriented and reactive, unable to take the initiative or carry out a coherent plan of action. Our actions foreclose enemy options to reverse our gains or alter the ultimate outcome of a conflict, and develop powerful self-fulfilling expectations of victory that demoralize the enemy while increasing coalition and domestic support.

Naval forces can provide sustained protection for joint and coalition forces ashore, creating a sanctuary from which they can operate at will against the enemy. We support joint and coalition forces ashore, securing vital sea and air lines of communication, establishing battlespace dominance in the littoral, and providing defensive capabilities, such as air superiority and theater ballistic missile defense. Just as important, we use offensive operations to protect forces by countering threats at their source, placing the enemy on the defensive, and degrading his ability to employ his forces.

As we have always done, we keep the vital seaborne logistics pipeline flowing throughout the joint campaign. During the 1991 Gulf War and every other large-scale conflict in this century, more than 95 percent of all material, supplies, and equipment sent to the theater went by sea. We protect strategic sealift and afloat prepositioning ships and logistics facilities critical for large-scale joint operations.

Finally, naval forces can remain on scene after the joint campaign concludes to enforce sanctions and to maintain a U.S. presence for regional stability. We prevent the need for yet another joint campaign by taking advantage of our self-sustaining endurance to keep combat credible forces in the region. Our most significant contribution well may be to prevent the next conflict entirely through our forward presence for engagement and deterrence.

Our Course for the 21st Century

Forward…From the Sea emphasizes that projecting influence and power ashore requires naval forces shaped for joint operations. *Joint Vision 2010* provides the template for joint combat operations in the 21st century and envisions future joint combat operations leveraging information superiority to execute dominant maneuver, precision engagement, full-dimensional protection, and focused logistics. These operational concepts were anticipated in large measure by *Forward…From the Sea*. In many areas the Navy is at the leading edge of *Joint Vision 2010* capabilities.

We will continue actively to develop and implement a wide range of technological and operational innovations. Our Fleet Battle Lab experiments will be a process by which we make vital contributions to these efforts. The fleet is our battle lab. We will test new ideas and equipment every time we deploy or get underway for a significant exercise.

Our innovation efforts will examine operational concepts and doctrine, how we organize and command our forces to carry out our missions, the capabilities of future systems and platforms, the manner in which we provide maintenance and supply support, and the education and training of our people. We will focus our innovation and modernization efforts in the following areas.

- Naval forces will be able to provide sea-based overt and covert surveillance, reconnaissance, and information warfare capabilities for joint forces, and sea-based command and control up to the Commander Joint Task Force level. Our forces will be integrated into networked command and control systems that provide a common tactical picture of the battlespace to all commanders and are fully interoperable with joint command and control systems. Our Cooperative Engagement Concept will provide an unprecedented level of battlespace awareness and combat power by linking the sensors and weapons systems of an entire force into a highly integrated network. We will achieve faster speed of command, closer joint integration, and enhanced means of ensuring the warrior has the right information in the optimum display for immediate action.

- We will be a full partner in developing new amphibious warfare concepts and capabilities for implementing the Marine Corps concept Operational Maneuver From The Sea (OMFTS). OMFTS emphasizes using the sea as a secure area from which to conduct ship-to-objective movement. We will have a vital role in OMFTS-style operations as part of a highly integrated sea-air-land combined-arms team. We will provide enhanced naval fires, force protection, command and control, surveillance and reconnaissance, and logistics support for Marines ashore—enabling the high-tempo operations envisioned by OMFTS.

- We will be capable of providing every type of joint fire the nation requires, throughout the battlespace and with the precision the operation dictates. We will deliver precision naval fires fully integrated as an element of joint combat power. Navy innovations, like networked command and control systems and cooperative engagement, are a significant step in this direction. We will be able to deliver a large volume of firepower through new ways of achieving very high aircraft sortie rates and new weapons and platforms for delivering joint fires. Emerging precision and information capabilities rapidly are making traditional views—that specific platforms (air, surface or subsurface) and specific types of ordnance (missile, bomb or shell) have specialized roles—obsolete. We will deliver integrated joint fires with enhanced range, lethality, accuracy, and timeliness from aircraft, ships, and submarines for any type of mission.

- Building upon our already robust information, air, and maritime superiority capabilities, we will provide integrated protection for joint and coalition forces. Naval defensive capabilities, such as theater air defense and ballistic missile defense, will be integrated with joint systems for maximum protection of the joint force. Our defensive capabilities will complement land-based systems and in some situations may be the only U.S. capabilities readily available, particularly in the opening phase of a crisis or conflict. We will enhance the range, lethality, and joint integration of our force-protection capabilities and enhance our ability to defeat sea-denial threats and dominate the littoral battlespace.

- We will increasingly be capable of providing secure afloat joint logistics support. Our logistics innovation efforts will enhance strategic sealift and seaborne logistics. These efforts also support Department of Defense initiatives to improve logistics support, such as the total asset visibility system and “just-in-time” logistics. We will seek alternatives to maintaining large quantities of spares and explore ways of enhancing the joint and commercial commonality of system components.

Conclusion

The Navy’s course for the 21st century set by *Forward…From the Sea* has proven to be the right one for executing our critical roles in all three components of the National Military Strategy and for conducting the future joint operations envisioned in *Joint Vision 2010*. We will maintain our ongoing process of technological and operational innovation that has put us on the cutting edge of future warfighting capabilities. Our Navy people—well-led, working as a team, and taking pride in our Navy—will be the source of these innovations. The imagination and initiative of individual Sailors have given our Navy a rich heritage of innovation. Our people will keep us on a steady course toward continued operational primacy as we enter the 21st century.

CHAPTER 10

U.S. NAVY:

INFORMATION WARFARE STRATEGIC PLAN

Information: A Resource and a Weapon

Information is transforming our world! We are surrounded by information and the machines that produce, process, store, and use it. All of the physical infrastructure upon which modern society relies, including electrical power grids, banking systems, public switched telephone networks, and oil and natural gas pipelines, depend upon the flow of information to function. The same is true of our military forces. Our combat, command and control, and intelligence systems are computer based and information-dependent; as are logistics, maintenance, personnel, and medical systems. This dependence on information is not new; we have always relied upon information, so much so that collecting, exploiting, disseminating, and protecting it have long been an integral part of military operations. What is new is the increased access to information brought about by technology and the ensuing need to ensure a degree of information superiority over potential adversaries.

Information technology has improved the ability to see, prioritize, assign, and assess information. It has and will continue to significantly impact military operations by providing military decision makers a level of insight never before achievable—or denying them the critical information upon which decisions will hinge. Differences in quality, integrity, accuracy, and speed of information transfer will determine the advantage in future operations and may very well determine outcomes. Ensuring the availability of information while denying it to an adversary will demand that the Navy place a high priority on information superiority.

Military activities performed in the Information Age and operations conducted in the domain of cyberspace will require that we develop the ability to conduct information operations or information warfare across the spectrum from peace to conflict and return. The target of this discipline will be the adversary's decision making ability. The target set will be comprised of information-dependent systems; and the objective, to impede the adversary's information flow, decision cycle, and battle timeliness while protecting our own.

Information operations will continue to evolve, pushed by technology, by opportunity, and by the threat they portend. The remainder of this publication will present the Navy Vision for IO/IW and the goals and strategies we will employ to bring it to fruition. It should be used as a guide for the evolution of Navy IO/IW to optimize the development, delivery, and maintenance of IO capabilities for the fleet.

Information Operations

For U.S. naval forces, technology has expanded our target set, improved our aimpoint, and provided alternative means for achieving national security objectives. Information technologies offer us the potential to manipulate or degrade information systems, attack sensor systems and networks, disrupt satellite functions, interdict power grids, or negate sensor-to-shooter links, all without firing a shot. This improvement in our ability to bring force to bear in so precise a manner supports the very essence of warfighting. These operations, concentrated in the information domain, are defined by the timeframe in which they occur; by the approval process required; and in the context of traditional military activities.

Information operations exploit the opportunities and vulnerabilities inherent in the dependence on information to support military activities. Information operations include actions taken to affect an adversary's information and information systems, and those taken to protect U.S. information, information based processes, and information systems. Its goal is to ensure U.S. forces may act to deter conflict. The Navy must be prepared, should deterrence fail, to gain and maintain information superiority over any potential adversary. The focus of IO/IW is on information-dependent systems, including weapons, infrastructure, command and control, computer, and associated network systems. These operations address hardware, software, and associated personnel.

Joint Vision 2010 and the Challenge of IW

Joint Vision 2010 provides us a vision of future warfare in which U.S. forces will enjoy full spectrum dominance by achieving total information superiority. The basis for this framework lies in the command and control and intelligence, along with other applications of new technology, which will transform the traditional military functions of maneuver, strike, protection, and logistics. These transformations are so powerful that the Joint Staff has presented them as emerging operational concepts for Dominant Maneuver, Precision Engagement, Full Dimensional Protection and Focused Logistics. Achieving the level of information superiority needed to facilitate this revolution in military operations requires the services to develop both offensive and defensive IW capabilities. These will transcend the strategic, operational, and tactical levels of warfare to include Military Operations Other Than War.

Offensive IW will employ traditional methods such as precision attacks to destroy adversary key command and control nodes, and non-traditional methods such as electronic intrusion into information networks to deny, deceive, or degrade the adversary decision process. Effective defensive IW will be our only guarantee that we can maintain information superiority in the face of similar attacks on our own information systems. Together, they will provide the leverage needed to implement Joint Vision 2010.

The unique nature of IW, the necessarily covert nature of certain offensive IW operations, and the wide range of possibilities for using IW to support military operations or as an alternative means of achieving national security goals, presents the very significant challenge of establishing IW applications for future integration in national policy. In the absence of a current policy, we will look to the CINC campaign plans to provide a means of resolving policy issues related to IW. A fully integrated IW plan will serve to surface the information needed to establish Rules of Engagement (ROE) and coordinate through an interagency process to reduce, if not eliminate, the need for going outside DoD once execution of the campaign begins. Progress in this vital warfare area must continue as national policy evolves.

Although there is a general mandate for DoD to protect the nation from foreign military attack, the unfamiliar nature of IW, difficulties in identifying "computer network attack," and existing laws will constrain DoD from taking an overly proactive role in defending the National Information Infrastructure (NII). Offensive IW suffers similar concerns. Until required mechanisms for planning and approving potentially sensitive operations are put in place, and the relationship between traditional military activities and covert operations are established, there will be no clear division of effort among government agencies. Resolution of these and related IW problems await an improved understanding of IW among all concerned parties. However, this does not translate to inaction or postponement of IW initiatives by DoD. The services will continue to lead the nation in the development of IW weapons, doctrine, organization, and training.

The Navy's IW Mission

The Navy's IW mission is to sustain information superiority across the continuum of peace, crisis, and conflict enabling and enhancing the ability of naval forces to successfully execute joint military operations. Time and time again, the Navy has answered the nation's call, with forward-deployed naval forces, to deter aggression, enhance regional stability, provide timely crisis response and—when necessary—conduct offensive combat operations from the sea.

Today, IW offers naval forces an array of precision strike weapons, opening up lucrative and previously inaccessible target opportunities and offering planners enhanced options for winning decisively in the information-dependent engagements of the future.

IW Functional Areas

Offensive IW [is] action taken to manipulate, deny, deceive, delay, and destroy an adversary's information, systems, and networks. defensive IW [is] action taken to protect friendly information from exploitation and attack by unauthorized entities or adversaries.

As in all warfare areas, commanders use their own sensors as well as off-board assets to develop a common operational picture of the battlespace. IW commanders use organic sensors for the planning, real-time execution, and IW re-attack options for offensive IW and to detect and defend against an adversary's efforts. This tactical information, along with information from other sensors, is injected into the analytical intelligence process and contributes to the formal support provided to the IW Commander.

The Threat Is Out There

The IW threat takes many forms. It takes material form by corrupting computer databases, overriding control systems, inserting malicious software, conducting classic jamming of sensors and control links, employing psychological and deceptive practices, and physically attacking, destroying, or disrupting critical links and control nodes. With the advent of IW, the geographic sanctuary traditionally enjoyed by the U.S. is all but gone. The threat posed by IW has reached across time and space to close the gap with potential adversaries.

In the evolving IW battlespace, connectivity to a global network provides comprehensive access for friends and foes alike. As our infrastructure and military forces become more interconnected, sanctuary vanishes.

The development and rapid proliferation of digital technology in sensors, weapons, communications, and C2 systems has rapidly increased and expanded the threat. While we must continue our focus on a few technologically advanced nations, we must also be concerned with every individual or group with military, political, or economic motivations who has access to even the most rudimentary computer and communications capabilities.

The threat to our infrastructure exists today with countless individuals, groups, and nations having the capability to attack across the continuum of peace, crisis, and conflict.

Principles for the Evolution of Navy IW

Navy IW will be conducted as an integral part of Joint Operations; or may be executed on a stand-alone basis as an enabler and enhancer of service capabilities; interoperability and adherence to standards are paramount.

We will exploit technology and leverage intelligence to support offensive and defensive IW functions.

We will build on existing fleet capabilities and maximize the use of our operational, organizational, and technological resources.

We will apply a system design philosophy of modifying installed shipboard and aircraft systems for offensive and defensive IW purposes, whenever possible.

IW equipment and expertise, supported by doctrine and appropriate rules of engagement, will be embedded in the force when required.

Credible, forward deployed naval forces offer unique opportunities to employ IW capabilities, stemming from their sustained presence in critical regions.

We will establish Navy IW as a formal naval warfare mission area.

We will apply a risk management philosophy to our defensive IW investments and efforts.

Evolution of Navy IW Organizations

The origins of the Battle Force IW Commander can be traced to the 1970s and 1980s when distinct staff EW and Cryptologic officers were elements of the

Battle Group Commander's staff. With the infusion of modern digital technology into communications, sensors, and weapons systems in the early 1990s, the duties of the staff EWO, Cryptologist and Deception Planner were integrated under the Space and Electronic Warfare Commander (SEWC) to provide mission area focus and synergy.

Recognizing the importance of C2 and counter-C2 during Desert Storm, the Joint Staff, and subsequently the Navy, reorganized to integrate and coordinate disparate warfare disciplines under the Command and Control Warfare Commander (C2WC). The C2WC's mission was to attack enemy C2 in order to isolate enemy commanders from their forces. The elements of C2W were then defined as Operations Security, Psychological Operations, Military Deception, Electronic Warfare, and Physical Destruction.

IW and C2W. The growing sophistication, expansion, and reliance on information technology in the mid 1990s made it apparent that the role of the C2WC needed to evolve and expand to incorporate the information process, whether human or automated. To support this, the C2WC concept was expanded to focus on the vulnerabilities and opportunities presented by our adversaries' dependence on information and information systems, as well as to protect our own forces from attack.

To support the evolution of IW in the operational arena, CNO reorganized in 1994, designating OPNAV N64 as the Director, Information Warfare and appointed COMNAVSECGRU as the Executive Agent (EA) for IW.

The Naval Information Warfare Activity (NIWA) was established in 1994 and designated a Reinvention

Laboratory to field state-of-the-art IW systems, assess the vulnerability of naval systems, and manage naval IW-related modeling and simulation efforts.

The Fleet Information Warfare Center (FIWC) was established in 1995 as the Navy's IW Center of Excellence to act as the Fleet CINC principal agent for developing IW tactics, techniques, procedures, and training. CNO designated FIWC as the single Navy point of contact for coordinating both offensive and defensive IW support to the fleet. FIWC is authorized appropriate liaison with all required agencies and commands. FIWC operates under the operational control (OPCON) of the FLTCINCs and the administrative control (ADCON) of CINCLANTFLT; and the Technical Control of COMNAVSECGRU for certain information systems security monitoring efforts. COMNAVSECGRU recently tasked NSGA Pensacola to support FIWC in the conduct of vulnerability assessments of automated systems.

A Navy IW Council, comprised of voting representatives from OPNAV N64, OPNAV N51, the Fleet CINCs, SPAWAR, and COMNAVSECGRU was formally established in February 1996. The IW Council considers all aspects of IW implementation in the Navy. Commanding officers of NIWA and FIWC attend the Navy IW Council of Captains' meetings.

In March 1996, the Space and Naval Warfare Systems Command (SPAWAR) reorganized, forming an Information and Electronic Warfare Directorate (PD-16) to develop and acquire IW Exploit, Attack, and Protect systems.

The IW Foundation...Reducing Our Greatest Risk

Naval forces are critically dependent on information-intensive systems to generate dominant combat power. Our growing dependence on information places vital demands upon its availability and integrity. Defense of our information and information systems against intrusion and attack must be made a priority in order to achieve information superiority. Recognizing this, the Secretary of the Navy, the Honorable John Dalton, outlined a comprehensive Defense IW program to achieve and sustain information assurance (the availability, confidentiality, and integrity of our information and information systems) for naval forces. This program constitutes a roadmap to increased security of the Navy Protected Information Environment (PIE).

- Identify information systems that are critical to our military effectiveness and national security. Designate these systems, in total, as the Protected Information Environment, or PIE. Focus INFOSEC efforts and investments on the PIE.

- Establish the means to model three critical aspects of PIE: (a) vulnerability of components and systems to attack; (b) consequences of different types of information attack; and (c) means of restoration from successful attacks.

- Apply the information developed from these analyses to the design of new systems, so as to minimize risk of intrusion on these systems and achieve the most “graceful degradation” if they are successfully attacked.

- Develop and maintain a consistent and rigorous risk and consequence management methodology for protecting existing systems and processes within the PIE. This methodology must balance threat, cost, and system criticality.
- Invest in methods and systems designed to enhance the probability that information attacks are promptly detected and their consequences rapidly assessed.
- Develop policy, strategy, and tactics for responding to attacks so as to deter and defend against further attacks and deceive as to the effects of attacks that have been conducted. Identify policy, legal, and administrative issues that present opportunities or obstacles in this effort. Develop plans to clarify or overcome them, as appropriate.
- Establish a Red Team to simulate attacks on DoN systems. Include simulated attacks, the contingency plans that would respond to them, and information warfare disaster recovery as a regular part of fleet and field exercise. Integrate information warfare defensive capability and vulnerabilities into readiness reporting systems.
- Establish appropriate counter-intelligence capabilities to cope with information warfare threats. As part of this effort, maintain and strengthen the closest ties to intelligence and law-enforcement organizations.

- Establish close liaison with civilian and other governmental organizations that are developing defensive information strategies and tactics. Place the highest priority on coordination with the other services and the National Security Agency in these respects.
- Provide support to IW R&D efforts, ensuring continuing access to the most advanced developments in tools and processes. Capitalize on the flexibility and leverage resulting from modern information technology by sharing technology and processes between the traditional attack and exploit disciplines.
- Ensure that DoN doctrine emphasizes information dominance in the battlespace. Implement effective technical and managerial training programs so that the DoN has sufficient personnel who are trained and skilled in network information systems administration and security.
- Institute a DoN-wide education and awareness effort focused on steps to increase information assurance and instituting best practices into Navy and Marine Corps Standard Operating Procedures.

Navy IW Strategic Action Areas

The following pages address specific courses of action for these Strategic Action Areas: Policy and Doctrine, Organization, Career Development, Training and Education, Research and Development, Acquisition, Mission Planning, and Simulation, [and] Intelligence Support.

Policy and Doctrine

Background: DoD Directive TS3600.1, information warfare, December 1992, established the foundation for all IW policy within DoD. JCS followed with MOP 30 in March of 1993 which integrated Psychological Operations (PSYOP), Military Deception, Operations Security (OPSEC), Electronic Warfare (EW), and destruction into a new warfare area, Command and Control Warfare. CNO issued OPNAVINST 3430.25, April 1994, which broadly outlined Navy IW policy. It was closely followed by an IW/C2W implementation instruction, OPNAVINST 3430.26 in January 1995. CJCS instruction 3210.01 defined Joint policy for IW. Joint Publication 3-13, Joint IW doctrine, is in draft.

*Desired Outcome: …*a powerful naval force guided by IW policy and doctrine which will have a decisive impact, from the sea, in times of peace, crisis, and conflict. To achieve this outcome we must develop IW policy and doctrine which:

- Ensures compatibility with evolving Joint policy and doctrine.
- Implements a dominant IW capability within the Navy.
- Emphasizes coherency and synergy between the offensive and defensive aspects of Navy IW.
- Recognizes and supports the critical role IW sensors play in providing precision information essential for offensive and defensive IW.

Course of Action: OPNAV will continuously review and revise IW related policies to ensure they authorize, enable, and guide research, development, acquisition, and maintenance of IW technologies, systems, and programs to support a superior naval offensive and defensive IW force.

OPNAV will develop, regularly update, and refine the Navy IW implementation plan to ensure it contains clear objectives, authorities, and accountabilities.

OPNAV and Naval Doctrine Command (NDC) will establish IW as a formal warfare area.

OPNAV will coordinate with NDC to ensure IW is included in the long term vision for the Navy as well as in current doctrine.

CNO/CMC will ensure complementary Navy and Marine Corps IW policy and doctrine.

Organization

Background: OPNAV Instruction 3430.26 contained implementation guidance and identified organizational relationships and responsibilities for IW. This instruction laid the foundation for Navy's IW organizational structure, doctrine, equipment procurement, and training which will ensure the successful conduct of Navy IW.

Desired Outcome: Development of well defined organizational responsibilities and inter-relationships that ensure the availability of superior IW capabilities to support naval forces.

Course of Action: Fleet CINCs establish a standardized IW commander and staff in the

Composite Warfare Commander (CWC) organization commensurate with increased IW mission and structured in consideration of the recent Joint Staff designation of the Operations Directorate J-3 (J-39) as the primary focal point for all IW operations.

OPNAV will, in coordination with the Fleet CINCs, refine the interrelationships and support requirements between the IW shore infrastructure and afloat IW organizations.

COMNAVSECGRU will formalize its technical control relationship to FIWC for defensive IW activities.

OPNAV, in coordination with the Commander, Naval Security Group Command, will investigate the concept of an IW Wing at NAS Whidbey Island, to focus VAQ, VQ, VPU, and NSGA Whidbey IW capabilities.

OPNAV will ensure IW expertise is resident on the CNO N3/N5 staff.

The Navy IW Council will make recommendations on IW implementation in the Navy.

OPNAV will establish a Flag Officer Steering Committee to review and approve recommendations for the conduct and implementation of IW within the Navy.

Career Development

Background: IW is a technologically intensive warfare area. It relies on many officer and civilian designations and enlisted ratings to bring necessary technical skills to the IW profession. Successful IW will rely on the development of knowledgeable IW professionals from all communities committed to integrating IW capabilities into all aspects of the Navy mission.

Related areas of expertise in space and command and control, when combined with IW professionals, make up the Space, IW, and C2 (SIWC2) professional resource pool. In addition, warfighters from all disciplines should take lessons learned from IW experience tours back to their own warfare community.

Desired Outcome:

- To develop a cadre of officer and enlisted personnel with requisite technical and operational skills to ensure our naval forces are capable of meeting Navy and Joint IW mission requirements.
- Establish an incentive and opportunity-based career path supported by a visible and viable personnel management process.

Course of Action: Director of Naval Training establish basic, intermediate, and advanced training and education opportunities, both service and Joint, to produce highly capable career IW professionals.

COMNAVSECGRU will establish a mechanism for managing officer, enlisted, and civilian personnel with fW expertise to ensure their technical and professional IW competency.

Primary manpower claimants will establish a career progression to produce officer, enlisted, and civilian personnel with the skills and experience required to advance to key senior leadership positions in Joint and service assignments within their designated warfare area as well as in the IW area.

Fleet CINCs, with assistance from COMNAVSECGRU, identify IW billet requirements to support Joint and Navy IW missions.

Deputy Chief of Naval Operations for Manpower and Personnel identify Navy personnel with the appropriate aptitude, training, education, and experience levels for assignment to Joint and Navy IW billets.

Deputy Chief of Naval Operations for Manpower and Personnel establish Navy officer Additional Qualification Designator (AQD) codes and assign them to IW billets and personnel for use in detailing personnel to all IW assignments.

Training and Education

Background: Technological change in information systems occurs at a startling rate. New products—hardware and software—are announced daily. As these products are integrated into military C2 and weapons systems and into government and civilian infrastructure, IW opportunities as well as vulnerabilities will constantly recur.

The speed of advance in modern information technology requires aggressive training and education approach to ensure Navy professionals keep pace with emerging technologies and are able to successfully meet Navy IW mission requirements.

Maintaining mastery of the IW Battle Space will require a level of responsiveness in our technical training that will be difficult to achieve via traditional classroom training. Therefore, Navy must consider alternative “non-traditional” training solutions such as Computer Based Training (CBT), Commercial Off-The-Shelf (COTS) packages, and specially-tasked quick reaction training efforts. While these approaches have superior potential for keeping pace with technological and operational advances, they also demand more management time and attention.

Desired Outcome:

- Provide all Navy personnel with an understanding of the importance of IW and an awareness of the opportunities and risks associated with the use of information technology.
- Establish a cadre of designated officer and enlisted personnel who are equipped with the required specialized skills to successfully perform Navy IW missions and functions.

Course of Action: Director of Naval Training establish broad-based IW curricula to be included in officer and enlisted career progression training. Ensure timely updates to IW training materials to stay abreast of IW technological and operational developments; pursue "nontraditional" education and training approaches that optimize and improve upon the responsiveness and timeliness of training.

Fleet CINCs include IW in Navy exercises, wargames, and predeployment evolutions to improve fleet IW skills.

Director of Naval Training expand IW tactics training at Tactical Training Groups, Atlantic and Pacific.

Naval Postgraduate School expand the IW curriculum to confront the challenge and anticipate the future.

Research and Development

Background: IW is characterized by a dynamic environment manifested in a variety of emerging technologies and applications. Naval warfighters require state-of-the-art technologies to stay ahead of our adversaries. The IW R&D process must proactively support the warfighter and must also be responsive and dynamic. The CNO staff will provide oversight of IW requirements and resources to ensure a common forum to drive IW R&D efforts.

Desired Outcome:

- A coordinated, aggressive R&D effort, supported by intelligence, that optimizes advancing technology and investments through "dual use" and interoperability.
- An IW R&D program that triggers revolutionary, threat responsive technology advances which can be rapidly integrated into the Joint warfighting environment.

Course of Action: OPNAV engage defense and national laboratories, defense colleges, civilian universities, engineering organizations, and commercial enterprises to expand the IW technology envelope.

OPNAV ensure other Service/Agency R&D activities are leveraged for Navy benefit; maximize the use of Commercial/ Government Off-The-Shelf (COTS/ GOTS) technologies.

OPNAV combine and integrate operational requirements with technology assessments to develop a dynamic and proactive IW R&D program which supports the warfighter.

Laboratories and agencies prioritize ongoing IW R&D efforts emphasizing the timeliness, confidentiality, authenticity, and protection of information as principal objectives to be preserved and attained in all system designs. Emphasize efforts to assess and mitigate own system vulnerabilities to an adversary's IW efforts while increasing our ability to exploit and attack adversary vulnerabilities.

Laboratories and agencies sponsor a continuing series of IW R&D and technology development seminars involving military, government, academia, and industry to exchange information and serve as a catalyst for expanding the IW technology envelope.

Acquisition

Background: IW system interoperability and effective integration of IW capabilities in the operating forces are critical. The Space and Naval Warfare Systems Command has established the Information and Electronic Warfare Program Directorate (PD 16) with two major objectives: adopt standards for all IW capabilities; and ensure Navy IW capabilities can be integrated forcewide and in a joint warfighting environment. The establishment of PD-16 consolidated the Navy acquisition agents for IW Protect (PMW 161), IW Attack (PMW 162), and IW Exploit (PMW 163).

Desired Outcome: A coordinated, requirements-driven Navy IW acquisition effort, supported by intelligence, that delivers integrated and embedded capabilities and systems meeting warfighter requirements for IW Protect, Attack, and Exploit.

Course of Action: Adopt/develop standards to minimize vulnerabilities, embed IW capabilities in the operating forces, and integrate capabilities in the Joint environment consistent with the Joint Requirement Oversight Council approved Mission Need Statement on IW.

All information intensive system developers conduct information vulnerability analyses during system design. In accordance with OPNAV and DASN (C4I) security standards, they will: focus on risk management and incorporating infon-nation security features during system design; test security features during development; review test results as part of milestone decision agent actions.

Incorporate technical architecture framework for information management standards, emphasize open architectures, and design naval information-intensive systems for maximum joint interoperability while preserving system security.

Invest specifically identifiable resources from information-intensive systems' programs for life cycle vulnerability assessments, analysis, and the acquisition of defensive system resources.

Develop formal relationships with the national intelligence community and other services to optimize contributions to IW capabilities assessments and development.

Systematically catalog Navy at-risk systems and drive prioritization of resource investments in concert with the Planning Programming and Budgeting System cycle and the FLTCINC requirements definition process.

Assess all information systems destined for forward deployed platforms for "dual use" potential as IW exploit and attack resources. Use exit criteria for acquisition milestones to reflect and aid adherence to this objective.

Expand Navy "Carry-On" programs which will enhance Quick Reaction Capabilities to rapidly respond to emergent offensive and defensive IW requirements.

Mission Planning and Simulation

Background: The success of IW operations is contingent upon planning, pre-mission rehearsal, and situational awareness. The tools which support this capability are resident in computer-based decision aids, primarily through Modeling and Simulation (M&S). Application of these techniques can greatly enhance the mission planning process by identifying and evaluating alternative courses of action, likely outcomes, unintended consequences, resource utilization and employment, and battle damage assessment.

IW Situational Awareness (SA) will furnish the warfighter with the information required to operate inside the enemy's decision cycle, while at the same time understanding his own vulnerabilities. The principal Navy vehicle for providing IW SA and mission planning is the Joint Maritime Command Information System (JMCIS). All tools developed within JMCIS will be compliant with the DII common operating environments, in effect, becoming IW shareware.

Desired Outcome:

- User-friendly, intuitive, and collaborative offensive and defensive IW SA displays, mission planning tools, and pre-mission rehearsal capabilities to serve Navy forces.

- Incorporate IW into the common operational picture and the Combat Direction System.

Course of Action: Within the structure of the DoD and DoN M&S planning guidance, initiate processes to participate in the development of M&S interoperability standards in the areas of:

- IW Acquisition Support. Concentrate on virtual prototyping, capabilities visualization/simulation tools, statistically-based and physics-based nodal, terrain, antenna, IW system models and analysis tools, and modeling of the IW battlespace to address consequences of and restoration from successful IW attacks.

- IW Assessment Support/Training Support. Build on IW acquisition/M&S support. Concentrate on IW mission planning to include: C2 nodes, links, and sensor data bases; C2 target capabilities, limitations, and vulnerabilities; and political and military leadership decision-making processes. Provide tailored computer graphics and visualization tools to support IW technical operations and mission rehearsals.

- IW Operations Support. In a forward deployed, JMCIS Flagship configuration, provide for planning and rehearsal of IW missions in a synthetic environment that accurately simulates expected terrain, environment, and threat considerations, as well as a synergistic display of red and blue C4I architectures and dependencies.

FIWC will take the lead in developing and consolidating fleet requirements for IW mission planning and tactical decision aid tools. Liaise with NIWA and other service IW centers to obtain IW M&S capabilities for FIWC and fleet training and planning missions.

NIWA will manage naval IW related M&S efforts with assistance from SPAWAR, service and national laboratories, and joint agencies as appropriate.

NIWA will take the lead in integrating detailed technical analysis and M&S methodology into acquisition, operation, and training of Navy IW systems and operators.

Intelligence Support

Background: IW requires that we modify traditional intelligence strategies and forge closer linkages between intelligence support, operations, and acquisition staffs to assure the best possible knowledge about potential enemies; to accommodate the technologies and dynamics of information systems, networks and uses; and to be able to understand the impact of IW on potential enemies.

Technology in the information domain is largely driven by the commercial sector. Accesses, applications, and services are in a continuous state of change. Significant leadtime is required to generate the intelligence necessary to develop offensive IW capabilities, to protect friendly information, and to target IW weapons. The full potential of the Navy's IW program cannot be realized without precise, timely, and technically credible intelligence. Commanders should develop operational requirements for IW that will drive intelligence support and capabilities development. The resultant long-term intelligence analysis may assist commanders in understanding how adversaries use and interpret information.

Desired Outcome:

- To provide accurate, timely intelligence on IW targets, information technology, and processes.

- Intelligence support must assist in Intelligence Preparation of the Battle Space and crisis end-game; accurately guide precision IW targeting; support IW research, development, and acquisition, and facilitate information assurance for naval forces.

Course of Action: Ensure Naval Intelligence support to IW is in consonance with Joint intelligence efforts including those at the Joint Staff, National Agencies, and Joint commands.

Define new essential elements of information to enhance critical support to Navy IW development and targeting objectives.

Identify intelligence support shortfalls and emergent requirements for Navy IW. While IW is highly technical and SIGINT dependent, it also requires all source intelligence to support perception management, PSYOP, and deception.

Examine technology developments and trends in information, automation, and networking. Ensure that they are characterized in intelligence products and databases.

Develop a cohesive approach to intelligence requirements, databases, and reporting to satisfy needs of operational commanders.

Vision for the Future

“The IW Vision: A Navy that will dominate the battlespace by achieving total information superiority using offensive and defensive information operations to preserve the peace, deter or resolve crisis, and fight and win in combat operations.”

This document attempts to capture the vision of a Navy guided by information warfare doctrine, manned by IW proficient sailors, and armed with an array of precision offensive and defensive IW weapons which enjoys a decisive ability to support the National Strategy across a spectrum of requirements. Advanced technologies, combined with smart targeting and the historic advantages of maneuver from the sea, will provide the Navy with unprecedented opportunities in its role as the premier forward deployed American military force. The growth and innovative application of technology will improve combat effectiveness, at the same time avoiding the vulnerabilities associated with increased information dependence.

The information revolution, driven by technology, is transforming society, reorienting economies, and transforming military operations. Navy recognized the potential of information in warfighting in the late 1980s, developed the Copernicus Strategy, and has never looked back. The key to continued development and progress will depend upon our ability to create an efficient organizational structure, energized by innovation and linked to technology, to realize the benefits of information operations. This strategic plan is intended to provide a comprehensive concept for the conduct of information operations/information warfare to enable Navy to support national security objectives and to meet the requirements of joint combat operations.

CHAPTER 11

OPERATIONAL MANEUVER FROM THE SEA:

A CONCEPT FOR THE PROJECTION OF NAVAL POWER ASHORE

In the white papers “From the Sea” and “Forward From the Sea,” the Secretary of the Navy, with the Chief of Naval Operations and Commandant of the Marine Corps, began the development of a new approach to naval operations. This approach places unprecedented emphasis on littoral areas, requires more intimate cooperation between forces afloat and forces ashore, introduces the concept of the naval expeditionary force, and provides the foundation for Operational Maneuver from the Sea.

Like its predecessor, the approach to amphibious warfare developed at Quantico during the 1930s, Operational Maneuver from the Sea is a response to both danger and opportunity. The danger, summarized by the phrase “chaos in the littorals,” consists of a world characterized by the clash of the myriad forces of national aspiration, religious intolerance, and ethnic hatred. The opportunity comes from significant enhancements in information management, battlefield mobility, and the lethality of conventional weapons.

These two changes to the operational environment, a new series of threats and enhanced tactical capabilities, are significant ones. While they change neither the nature of war nor our fundamental doctrine of maneuver warfare, “chaos in the littorals” and the military applications of new technologies will have a profound effect on where we fight, who we fight, and how we fight. This, in turn, will require considerable alterations in the education of leaders, the organization and equipment of units, and the selection and training of Marines.

The details of these alterations are, as yet, unknown. Refocusing the Marine Corps to meet the needs of the next century will, like all successful military innovation, involve a great deal of debate and experimentation….And, if history is any guide, the conclusions we draw from this process may well bear little resemblance to the assumptions with which we started.

“Chaos in the Littorals”: Challenge and Opportunity

In the future, the United States is likely to face a number of very different threats to its security, interests, and way of life. Many of these will be associated with the littorals, those areas characterized by great cities, well-populated coasts, and the intersection of trade routes where land and sea meet. While representing a relatively small portion of the world’s surface, littorals provide homes to over three-quarters of the world’s population, locations for over 80 percent of the world’s capital cities, and nearly all of the marketplaces for international trade. Because of this, littorals are also the place where most of the world's important conflicts are likely to occur.

Close association with the littorals is one of the few things that conflicts of the near future are likely to have in common. In all other respects—goals, organizations, armament, and tactics—the warfare of the next 20 years will be distinguished by its great variety. For that reason, it is imperative that the Marine Corps resist the temptation to prepare for only one type of conflict. To focus on one threat, greatly increases the danger that we will be surprised, and perhaps defeated, by another.

To influence events overseas, America requires a credible, forwardly deployable, power projection capability. In the absence of an adjacent land base, a sustainable forcible entry capability that is independent of forward staging bases, friendly borders, overflight rights, and other politically dependent support can come only from the sea. The chaos of the future requires that we maintain the capability to project power ashore against all forces of resistance, ranging from overcoming devastated infrastructure to assisting a friendly people in need of disaster relief to countering the entire spectrum of armed threats.

The Breakdown of Order

The most obvious challenge faced by the United States and its Marine Corps is the worldwide breakdown of order. From the former Soviet Union to the former Yugoslavia, from the Atlas Mountains of North Africa to the Andes of South America, and from the streets of Washington, D.C. to the streets of Algiers, governments are losing their monopoly on organized violence. The result, as Marines have seen in Somalia, Lebanon, and Los Angeles, will be chaotic situations in which ethnic groups, street gangs, clans, and other non-state actors wage the war of “all against all.”

In many parts of the world, this trend towards the breakdown of order is likely to continue. Loyalty will shift, as it has for some time, from states to more intimate groupings, and from organizations that can keep the peace to entities that do a far better job at providing people with a sense of purpose and community. The long-term implications of this realignment of allegiances is hard to gauge. In the immediate future, however, we can be sure of more of the same sort of chaos—famine, terrorism, crime—that we see in our newspapers every day.

One particularly frightening possibility is the use of weapons of mass destruction by non-state actors. States that fail to command the loyalty of significant portions of their population will have difficulty controlling their stockpiles of nuclear, biological, and chemical weapons.

Non-state actors that cannot access traditional means of mass destruction may contemplate such equally destructive expedients as the blowing up of dams and the poisoning of water supplies. Even without weapons of mass destruction, non-state actors wield considerable destructive power. They can disrupt economies to the point of famine and societies to the point of lawlessness.

Regional Powers

The breakdown of order is not a universal phenomenon. Many areas of the world will continue to be dominated by states whose armed forces, while not always armed with the most advanced weaponry, are still formidable opponents. Regional powers that acquire, as many are likely to, nuclear weapons and other weapons of mass destruction will become even more powerful.

Regional powers are not necessarily hostile. Indeed, much of America's foreign policy is based upon alliances with regional powers. Nonetheless, a change of regime, a shift in the international balance of power, or even the perception of opportunity can turn a neutral or even friendly regional power into a hostile one….

The Next Superpower

At present, the United States is the only superpower in the world. If history is any guide, this enviable position is unlikely to be permanent. At some time in the future, another superpower—whether an existing state, a new state, or an alliance of states—could rise up.

It is unlikely that this new superpower will be a mirror image of the United States. Nonetheless, the advantages so evident in our recent conflicts with regional powers—superior numbers, logistics, wealth, and technology—are likely to be matched by similar advantages in the hands of our rival. It is even possible that the new superpower will possess more of the basic building blocks of military power than we will. In such a situation, the outcome will depend, to a degree unprecedented in recent history, upon the skill with which we fight.

Whether our enemy is a superpower as large and as rich as we are, or a regional power armed with second-hand weapons, or a political entity that has neither a capital city nor coinage, the wars of the near future share a number of important characteristics. Many of these derive from the wide availability of a variety of weapons that are far more lethal than the weapons used for most of the 20th century. These weapons include existing precision-guided munitions; non-line of sight gunner-in-the-loop weapons such as the fiber-optic guided missile; and improved level-of-effort munitions rockets/missiles, artillery, and mortars.

In war against non-state actors, where the proximity of innocents is often the enemy's greatest advantage, and in operations other than war, more precise weapons will allow a significantly greater degree of discrimination. A guided missile sent through a window, an armed robot turning a corner, and a directed energy weapon covering an exit will often be useful in situations where the delivery of tons of high explosive would be counter-productive.

In a war against regional powers, more precise weapons, whether precision-guided or level-of-effort, will allow greater effect on the target for far fewer rounds. This translates into additional shipping space available for landing force requirements, reductions in overland transport, and reductions in on-shore storage. The reduced logistics footprint of landing forces armed with more precise weapons will also translate into a significant reduction in the time needed for ship-to-objective and shore-to-ship maneuver.

In a war against a new superpower, new technologies will allow us to compete on equal terms. The infrastructure of 20th century combat power—large dumps of fuel and ammunition, ships waiting for days to unload their cargoes, and crowded assembly areas—will make lucrative targets for the weapons of the 21st century. At the same time, landing forces armed with the C2, tactical mobility, and fire support capabilities of the present will be hard pressed to decisively engage an enemy who is likely to combine the destructive capability of a conventional force with the elusiveness of a guerrilla.

New technologies, whether organic or in support, will give small units unprecedented combat power. Since small units are easier to move than large ones, these new technologies will permit high tempo operations in and between a wide variety of environments. At the same time, new weapons, which will inevitably be wielded by at least some of our enemies, require that our units be hard to detect, far-ranging, and fast-moving.

Responding to the Challenge

There is no single answer to the many challenges that will present themselves in the future. Naval forces will have to adapt as they have done throughout history to changing circumstances. For that reason, it is important that naval forces avoid a narrow definition of their capabilities. At the same time, the fact that the future is uncertain is no excuse for failing to make adequate preparations.

The centerpiece of our preparations for the future is an approach to expeditionary, littoral, and amphibious warfare known as Operational Maneuver from the Sea. While Operational Maneuver from the Sea will not define all Navy/ Marine operations, the attitudes, skills, techniques and equipment associated with it will provide naval forces with a solid foundation for future improvisation.

The heart of Operational Maneuver from the Sea is the maneuver of naval forces at the operational level, a bold bid for victory that aims at exploiting a significant enemy weakness in order to deal a decisive blow. Mere movement, which may lead to indecisive results or even be counterproductive, does not qualify as operational maneuver. That is to say, operational maneuver should be directed against an enemy center of gravity—something that is *essential* to the enemy's ability to effectively continue the struggle.

The center of gravity may be a physical object (a military force, a city, a region) or a source of supplies or money. More often than not, the center of gravity will be an intangible, essential element of the political and moral forces that keep our enemies in the fight against us. The purpose of the legitimate use of force, is to convince our enemies that it is unwise and, in the final analysis, wrong to make war against us.

The search for decisive effect is common to all forms of operational maneuver, whether on land, at sea, or in the littorals where land and sea meet. What distinguishes Operational Maneuver from the Sea from all other species of operational maneuver is the extensive use of the sea as a means of gaining advantage, an avenue for friendly movement that is simultaneously a barrier to the enemy and a means of avoiding disadvantageous engagements. This aspect of Operational Maneuver from the Sea may make use of, but is not limited to, such techniques as sea-based logistics, sea-based fire support and the use of the sea as a medium for tactical and operational movement.

For most of the 20th century, the usefulness of sea-based logistics was limited by the voracious appetite of modem landing forces for such items as fuel, large caliber ammunition, and aviation ordnance. As a result, the options available to landing forces were greatly reduced by the need to establish, protect, and make use of supply dumps. Concerted efforts were delayed and opportunities for decisive action missed while the necessary supplies accumulated on shore.

In the near future, improvements in the precision of long-range weapons, greater reliance on sea-based fire support, and, quite possibly, a decrease in the fuel requirements of military land vehicles promise to eliminate, or at least greatly reduce, the need to establish supply facilities ashore. As a result, the logistics tail of landing forces will be smaller, ship-to-shore movement will take less time, and what were previously known as "subsequent operations ashore" will be able to start without the traditional "build up phase." In other words, landing forces will move directly from their ships to their objectives, whether those objectives are located on the shoreline or far inland.

The significant reduction of logistics infrastructure ashore will also facilitate the rapid re-embarkation of the landing force. This will enable the landing force to avoid combat offered on unfavorable terms, to avoid obstacles that stand in the way of decisive action, and to make use of the inevitably perishable advantage of surprise. In effect, powerful landing forces will be able to do what had hitherto been the exclusive province of lightly armed landing parties.

When combined with a command and control system oriented towards rapid decision-making at all levels of command, the additional speed and flexibility offered by these new techniques translates into a high tempo of operations. Vulnerabilities can be exploited before they are reduced, opportunities seized before they vanish, and traps sprung before they are discovered. In short, we will be able to act so quickly that the enemy will not be able to react effectively until it is too late.

Setting the Course to Make It Happen

Operational Maneuver from the Sea requires that we focus our efforts on those areas which afford us the greatest return. Specifically, we must improve our operations, modernize our capabilities, and strengthen our intellectual underpinnings.

Directions

OMFTS requires significant changes in the way we are organized, in the way we move between the sea and the objective, and the way we deal with the wide variety of missions we will be called upon to support.

Organization. OMFTS treats the littoral as a single environment in which the cooperation of units on land, at sea, and in the air is based on a shared vision of what must be done, intimate knowledge of the capabilities and weaknesses of each type of unit, and an *esprit de corps* that transcends service identity or occupational specialty. This can only be achieved if the naval expeditionary force is organized and trained as a highly cohesive team.

Movement Between Land and Sea. OMFTS requires rapid movement, not merely from ship to shore, but from ship to objectives that may be miles away from blue water and from inland positions back to offshore vessels. While some operations may require the establishment of bases ashore, the practice of separating ship-to-shore movement from the tactical and operational maneuver of units ashore will be replaced by maneuvers in which units move, without interruption, from ships at sea to their inland objectives.

The Spectrum of Conflict. In contrast to previous approaches to amphibious warfare, OMFTS is not limited to the high end of the spectrum of conflict. Indeed, in a world where war will be made in many different ways, the very notion of "conventional" warfare is likely to fall out of use. For that reason, the techniques of OMFTS must be of use in a wide variety of situations, ranging from humanitarian relief to a high-stakes struggle against a rising superpower.

Capabilities

Operational Maneuver from the Sea will require us to overcome challenges in the areas of battlefield mobility, intelligence, command and control, fire support, aviation, mine countermeasures, and sustainment. In evolving OMFTS, we will meet these challenges and find solutions using both technology and new approaches in doctrine, organization, tactics, and training.

Mobility. To move units from ships lying over the horizon to objectives lying far from the shore, we will require the capability to cross great distances, reduce the limitations imposed by terrain and weather, and, most importantly, to seamlessly transition from maneuvering at sea to maneuvering ashore and vice-versa.

Intelligence. The high tempo of operations essential to successful OMFTS requires that intelligence be provided to decision makers with a minimum of delay. Technology that permits the rapid dissemination of intelligence products will play an important role in this effort. However, the key to effective intelligence support of OMFTS, lies in the orientation of intelligence specialists. In particular, intelligence specialists must be capable of rapidly making educated judgments about what the enemy is likely to do.

Command and Control. The command and control system best suited to OMFTS will be very different from those developed to deal with previous approaches to amphibious warfare. Techniques previously employed to compensate for the inability of fire support units to see the battlefield will give way to techniques that exploit the fact that combatant units will be better informed than ever before. Communications systems designed to provide a few headquarters with an overall view of the situation will have to be replaced by those that provide units with control over the information they need. The equipment to make this transition from communications nets to information networks has already been developed. Making this new technology work will require fundamental changes to the skills and attitudes possessed by Marines involved with the command and control system. The key to this capability lies more in the realm of education and doctrine than it does in the realm of hardware.

Fires. Successful execution of OMFTS will drive changes in fire support. To improve our mobility ashore, we will increasingly take advantage of sea-based fires and seek shore-based fire support systems with improved tactical mobility. To support rapidly maneuvering forces, we must streamline our fire support coordination procedures to improve responsiveness. To provide effective fires, forces afloat and ashore require the ability to deliver fires with increased range and improved accuracy and lethality. Finally, we will use fires to exploit maneuver just as we use maneuver to exploit the effects of fires.

Aviation. Our combat aircraft must be capable of operating from a variety of ships and austere bases ashore, perform a variety of missions, and land on a wide variety of surfaces. Our aviation units must be organized, trained, and employed as integral parts of a naval expeditionary force.

Mine Countermeasures. Because of their relative low cost and pervasiveness, mines have become a cheap means of limiting the mobility of ships and landing craft in the contested littoral regions. For that reason, we must develop and enhance our counter-mine/ obstacle reconnaissance, mine marking and clearing capabilities, precision navigation, and in-stride breaching to support maneuver at sea, ashore, and during the transition from sea to land.

Combat Service Support (CSS). The requirement to sustain fast-moving, powerful, combined arms forces conducting ship-to-objective maneuver will strain the best logistics system. Speed and mobility comparable to the assault forces’ will be necessary for CSS elements responding to the dynamic demands of OMFTS. CSS flow must be efficient, secure, and timely, with the option to remain sea-based or to buildup support areas ashore. Delivery means and material handling demands are great, as is the need for a command and control system capable of rapidly communicating requirements and flexibly managing “right time, right place” support.

Foundations

Doctrine. The doctrine of maneuver warfare is fully compatible with the concept of Operational Maneuver from the Sea. On the other hand, many of the techniques and procedures currently used by Fleet and Fleet Marine Force units must be replaced by techniques that are more in accord with OMFTS. This is particularly true in the areas of fire support, logistics, command and control, and ship-to-objective maneuver.

Training and Education. The effective employment of OMFTS will necessitate changes in Marine Corps training and education programs. The operational environment for OMFTS is characterized by a dynamic, fluid situation. In such a chaotic situation, we require leaders and staffs who can tolerate ambiguity and uncertainty and make rapid decisions under stress. Producing leaders, from the small unit level to the MAGTF commander, who have the *experience* to judge what needs to be done and *know* how to do it can be accomplished only with an extensive amount of training and exposure to operational problems. We must have leaders who can operate effectively in spite of risks and uncertainty; we can develop these leaders by improving their capacity to identify patterns, seek and select critical information, and make decisions quickly on an intuitive basis. This intuitive-based decisionmaking cycle will be enhanced by extensive investments in education, wargaming and combat simulation activities, and battlefield visualization techniques. These investments will produce leaders who can make informed judgments, take decisive action, and thus ensure that OMFTS can be successfully executed.

Conclusion: The Future of Naval Warfare

Just as a littoral is formed by the meeting of land and sea, Operational Maneuver from the Sea is a marriage between maneuver warfare and naval warfare. From maneuver warfare comes an understanding of the dynamic nature of conflict, the imperative of decisive objectives, and the requirement for skillful operations executed at a high tempo. From naval warfare are derived a deep appreciation for the strategic level of war, the advantages inherent in sea-borne movement, and the flexibility provided by sea-based logistics. Operational Maneuver from the Sea will couple doctrine with technological advances in speed, mobility, fire support, communications, and navigation to seamlessly and rapidly identify and exploit enemy weaknesses across the entire spectrum of conflict. When properly united, these elements of Operational Maneuver from the Sea provide the United States with a naval expeditionary force that, while deployed unobtrusively in international waters, is instantly ready to help any friend, defeat any foe, and convince potential enemies of the wisdom of keeping the peace.

CHAPTER 12

REPORT OF THE QUADRENNIAL DEFENSE REVIEW

By
William S. Cohen

The Secretary's Message

During the past decade, the world witnessed rapid and dramatic change. The Soviet empire disintegrated. The Iron Curtain dissolved. The Berlin Wall was dismantled. America no longer was engaged in a global competition with an ideological enemy. Where dictatorship once prevailed, democratic institutions now flourish and market economies are embraced by freedom-loving people throughout most of the industrial world.

The American people have much to celebrate over this turn of events, and there is every temptation to relax and take comfort in the preservation of tranquillity at home and the triumph of our values abroad. The flush of euphoria, however, must be tempered with the knowledge that while the prospect of a horrific, global war has receded, new threats and dangers—harder to define and more difficult to track—have gathered on the horizon….

It is commonly held—but erroneous—notion that America's military establishment and forces are trapped hopelessly in the past, still structured and struggling to fight yesterday's wars.…

Where We Are

Since 1985, America has responded to the vast global changes by reducing its defense budget by some 38 percent, its force structure by 33 percent, and its procurement programs by 63 percent.…

In making these reductions, we have carefully protected the readiness of our military to carry out its currently assigned missions. But it has become clear that we are failing to acquire the modern technology and systems that will be essential for our forces to successfully protect our national security interests in the future.…

Where We Are Going

…Building on the President's National Security Strategy, we determined that U.S. defense strategy for the near and long term must continue to shape the strategic environment to advance U.S. interests, maintain the capability to respond to the full spectrum of threats, and prepare now for the threats and dangers of tomorrow and beyond. Underlying this strategy is the inescapable reality that as a global power with global interests to protect, the United States must continue to remain engaged with the world, diplomatically, economically, and militarily.

…The information revolution is creating a Revolution in Military Affairs that will fundamentally change the way U.S. forces fight. We must exploit these and other technologies to dominate in battle. Our template for seizing on these technologies and ensuring military dominance is *Joint Vision 2010*, the plan set forth by the Chairman of the Joint Chiefs of Staff for military operations of the future.…

The path we have chosen strikes a balance between the present and the future, recognizing that our interests and responsibilities in the world do not permit us to choose between the two. This approach retains sufficient force structure to sustain American global leadership and meet the full range of today's requirements. At the same time, it invests in the future force with a focused modernization plan that embraces the Revolution in Military Affairs, and introduces new systems and technologies at the right pace.…

What's New?

First, the shape-respond-prepare strategy defined in the QDR process builds on the strategic foundation of past reviews and our experience since the end of the Cold War. We have determined that U.S. forces must be capable of fighting and winning two major theater wars nearly simultaneously.…We have also carefully evaluated other factors, including placing greater emphasis on the continuing need to maintain continuous overseas presence in order to shape the international environment and to be better able to respond to a variety of smaller-scale contingencies and asymmetric threats.

The QDR has also placed much greater emphasis on the need to prepare now for the future, in which hostile and potentially hostile states will acquire new capabilities. This demands increased and stable investment in modernization in order to exploit the revolution in technology and to transform the force towards *Joint Vision 2010*. We must fundamentally reengineer our infrastructure and streamline our support structures by taking advantage of the Revolution in Business Affairs that has occurred in the commercial world.

Second, our future force will be different in character. The programs we are undertaking now to exploit the potential of information technologies and leverage other advancing technological opportunities will transform warfighting. New operational concepts and organization arrangement will enable our joint forces to achieve new levels of effectiveness across the range of conflict scenarios.

Joint Vision 2010 describes four new operational concepts [dominant maneuver, precision engagement, full-dimensional protection, and focused logistics]. Together, they promise significant advantages in any operation or environment, something we call "full spectrum dominance." At the heart of the joint vision is information superiority—the ability to collect and distribute to U.S. forces throughout the battlefield an uninterrupted flow of information, while denying the enemy's ability to do the same.

In sum, we will continue to seek the best people our nation can offer and equip them with the best technology our scientists and engineers can produce. This technology will transform the way our forces fight, ensuring they can dominate the battlefield with a decisive advantage at all times across the full spectrum of operations from peacekeeping and smaller scale contingencies to major theater war. The key to success is an integrated "system of systems" that will give them superior battlespace awareness, permitting them to dramatically reduce the fog of war.

This system of systems will integrate intelligence collection and assessment, command and control, weapons systems, and support elements. It will connect the commanders to the shooters and suppliers and make available the full range of information to both decision makers in the rear and the forces at the point of the spear.

Achieving such capabilities is not an easy task and cannot be done in one leap. It is a step-by-step process involving the development of new technologies, investment in new platforms and systems, new concepts, training and doctrine, and formation of new organizational structures. But these are not just ideas, we have already started down the road and we have tangible results.

What's Next—How Do We Get From Here To There?

The first and most visible aspects of our overall plan to rebalance our defense programs are necessary modest reductions in military end strength and force structure. These reductions are offset in part by enhanced capabilities of new systems and streamlined support structures.…

Modernization of our forces depends upon a strong backbone of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems. The important and central role of these systems, and the large resources that must be devoted to them, inspired a hard and sweeping look at our entire effort devoted to C4ISR. The general focus and amount of resources devoted to this effort were determined to appropriate. We made a similar study of munitions programs and found that there is a high payoff for large investment we are making in precision weapons and that the focus of the programs and the scale of effort are appropriate.…

We also need to take advantage of business process improvements being pioneered in the private sector. Over the past decade, the American commercial sector has reorganized, restructured, and adopted revolutionary new business and management practices in order to ensure its competitive edge in the rapidly changing global marketplace. It has worked. Now the Department must adopt and adapt the lessons of the private sector if our armed forces are to maintain their competitive edge in the rapidly changing global security arena.…

Design, Approach, and Implementation of the Quadrennial Defense Review

As the fourth comprehensive review of our military since the end of the Cold War, the Quadrennial Defense Review (QDR) builds on our experience with the policy and forces of the 1991 Base Force Review, the 1993 Bottom-Up Review (BUR), and the 1995 Commission on Roles and Missions of the Armed Forces (CORM).…

…The Department of Defense designed the QDR to be a fundamental and comprehensive examination of America’s defense needs from 1997 to 2015: potential threats, strategy, force structure, readiness posture, military modernization programs, defense infrastructure, and other elements of the defense program. The QDR is intended to provide a blueprint for a strategy-based, balanced, and affordable defense program.…

The Global Security Environment

As the 21st century approaches, the United States faces a dynamic and uncertain security environment replete with both opportunities and challenges. On the positive side of the ledger, we are in a period of strategic opportunity. The threat of global war receded and our core values of representative democracy and market economics are embraced in many parts of the world, creating new opportunities to promote peace, prosperity, and enhanced cooperation among nations. The sustained dynamism of the global economy is transforming commerce, culture, and global interactions.…In fact, many in the world see the United States as a security partner of choice.

Nevertheless, the world remains a dangerous and highly uncertain place, and the United States likely will face a number of significant challenges to its security between now and 2015.

First, we will continue to confront a variety of regional dangers. Foremost among these is the threat of coercion and large-scale, cross-border aggression against U.S. allies and friends in key regions by hostile states with significant military power.…

Between now and 2015, it is reasonable to assume that more than one aspiring regional power will have both the desire and the means to challenge U.S. interests militarily.

In addition, failed or failing states may create instability, internal conflict, and humanitarian crises, in some cases with regions where the United States has vital or important interests….

Second, despite the best efforts of the international community, states find it increasingly difficult to control the flow of sensitive information and regulate the spread of advanced technologies that can have military or terrorist uses. The proliferation of advanced weapons and technologies will continue. This could destabilize some regions and increase the number of potential adversaries with significant military capabilities, including smaller states and parties hostile to the United States, and change the character of the military challenges that threaten our national security….

Third, as the early years of the post-Cold War period portended, U.S. interests will continue to be challenged by a variety of transnational dangers, and the lives of U.S. citizens will often be placed at risk, directly and indirectly….

Fourth, while we are dramatically safer than during the Cold War, the U.S. homeland is not free from external threats. In addition to the threat inherent in the strategic nuclear arsenals of other countries, there is the potential for further spread of intercontinental ballistic missiles and weapons of mass destruction. In addition, other unconventional means of attack, such as terrorism, are no longer just threats to our diplomats, military forces, and private Americans overseas, but will threaten Americans at home in the years to come. Information warfare (attacks on our infrastructure through computer-based information networks) is a growing threat.

Indeed, U.S. dominance in the conventional military arena may encourage adversaries to use such asymmetric means to attack our forces and interests overseas and Americans at home.…If…an adversary ultimately faces a conventional war with the United States, it could also employ asymmetric means to delay or deny U.S. access to critical facilities; disrupt our command, control, communications, and intelligence networks; deter allies and potential coalition partners from supporting U.S. intervention; or inflict higher than expected U.S. casualties in an attempt to weaken our national resolve.

Areas in which the United States has a significant advantage over potential opponents and increasing capabilities (e.g., space-based assets; command, control, communications, and computers; and intelligence, surveillance, and reconnaissance) could also involve inherent vulnerabilities that could be exploited by potential opponents (e.g., attacking our reliance on commercial communications) should we fail to account for such challenges.…

Defense Strategy

Since the founding of the Republic, the United States has embraced several fundamental and enduring goals as a nation: to maintain the sovereignty, political freedom, and independence of the United States, with its values, institutions, and territory intact; to protect the lives and personal safety of Americans, both at home and abroad; and to provide for the well-being and prosperity of the nation and its people.…

Key Tenets of U.S. National Security Strategy

How can we best achieve these national security goals and preferred international conditions in today's changing, uncertain, and still dangerous world?

In recent years people have expressed views on this question spanning the political and ideological spectrum. At one end of the spectrum, it can be argued that because we no longer face the challenge of a global peer competitor like the Soviet Union, we would be best served as a nation by focusing our energies at home and only committing military forces when our nation's survival is at stake.…

At the other end of the spectrum is the argument that as the world's only remaining superpower, the United States has significant obligations that go well beyond any traditional view of national interest, such as generally protecting peace and stability around the globe, relieving human suffering wherever it exists, and promoting a better way of life, not only for our own citizens but for others as well.

In between these competing visions of isolation and world policeman lies a security strategy that is consistent with our global interests—a national security strategy of engagement. A strategy of engagement presumes the United States will continue to exercise strong leadership in the international community, using all dimensions of its influence to shape the international security environment.…

Maintaining a strong military and the willingness to use it in defense of national and common interests remain essential to a strategy of engagement as we approach the 21st century. Today, the United States has unparalleled military capabilities….To sustain this position of leadership, the United States must maintain ready and versatile forces capable of conducting a wide range of military activities and operations—from deterring and defeating large-scale aggression, to participating in smaller-scale contingencies, to dealing with asymmetric threats like terrorism….

The Defense Strategy

In order to support this national security strategy, the U.S. military and the Department of Defense must be able to help shape the international security environment in ways favorable to U.S. interests, respond to the full spectrum of crises when directed, and prepare now to meet the challenges of an uncertain future. These three elements—shaping, responding, and preparing—define the essence of U.S. defense strategy between now and 2015.

Shaping The International Environment. In addition to other instruments of national power, such as diplomacy and economic trade and investment, the Department of Defense has an essential role to play in shaping the international security environment in ways that promote and protect U.S. national interests. Our defense efforts help to promote regional stability; prevent or reduce conflicts and threats, and deter aggression and coercion on a day-to-day basis in many key regions of the world….

DoD's role in shaping the international environment is closely integrated with our diplomatic efforts. On a daily basis, our diplomatic and military representatives work together towards U.S. objectives in all regions of the world. In times of crisis, diplomacy is a critical force multiplier when the United States seeks and works with coalition partners and requires access to foreign bases and facilities. Conversely, diplomacy is frequently enhanced when it is supported by the potential for a military response.

Responding to the Full Spectrum of Crises. Despite our best efforts to shape the international security environment, the U.S. military will, at times, be called upon to respond to crises in order to protect our interests, demonstrate our resolve, and reaffirm our role as a global leader. Therefore, U.S. forces must also be able to execute the full spectrum of military operations, from deterring an adversary's aggression or coercion in crisis and conducting concurrent smaller-scale contingency operations, to fighting and winning major theater wars.

Although the United States will retain the capabilities to protect its interests unilaterally, we often find advantages to acting in concert with like-minded nations when responding to crises….As the U.S. military incorporates new technologies and operational concepts at a pace faster than that of any other military, careful design and collaboration will be needed to ensure we meet new interoperability challenges….

*Preparing Now for an Uncertain Future….*Our commitment to preparing now for an uncertain future has four main parts:

- **Pursue a Focused Modernization Effort.** Fielding modern and capable forces in the future requires aggressive action today. Just as U.S. forces won the Gulf War with weapons that we developed many years before, tomorrow's forces will fight with weapons that are developed today

> and fielded over the next several years.… Sustained, adequate spending on the modernization of the U.S. forces will be essential to ensuring that tomorrow's forces continue to dominate across the full spectrum of military operations.
>
> - **Exploit the "Revolution in Military Affairs."** Our modernization effort is directly linked to the broader challenge of transforming our forces to retain our military superiority in the face of changes in the security environment and in the art of warfare. Just as earlier technological revolutions have affected the nature of conflict, so too will the technological change that is so evident today. This transformation involves much more than the acquisition of new military systems. It means harnessing new technologies to give U.S. forces greater military capabilities through advanced concepts, doctrine, and organizations so that they can dominate any future battlefield.

Because U.S. forces are committed every day to meeting the serious security demands of the present, transforming them must necessarily be a process of responsible evolution toward revolutionary capabilities. For several years, the U.S. military and DoD have been engaged in a variety of efforts to exploit the RMA. *Joint Vision 2010* has been key among these, stating that our joint forces can realize the potential of the RMA if we create and exploit information superiority to achieve full spectrum dominance through the synergy of four new operational concepts: dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. Achieving this full spectrum dominance means continuing to build an integrated, complex set of systems, especially a common command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture to achieve dominant battlespace awareness. Important complementary efforts include:

- the development of combatant commanders' and Service visions of warfare for 2010 and beyond;
- investment in an array of science and technology programs as well as exploratory research to identify, develop, and test innovative operational concepts and force configurations that exploit new technologies;
- practical experiments being conducted by each of the Services to test new concepts and capabilities. (These experiments are the process for developing new doctrines, tactics, training, and organizational structures to fully exploit the synergy brought to the battlefield by new technologies.)

In the next several years, DoD will seek to further strengthen both the culture and the capability to develop and exploit new concepts and technologies in order to make our forces more responsive to an uncertain world.

- **Exploit the "Revolution in Business Affairs."** A Revolution in Business Affairs also has begun. Efforts to reengineer the Department's infrastructure and business practices must parallel the work being done to exploit the Revolution in Military Affairs if we are to afford both adequate investment in preparations for the future, especially a more robust modernization program, and capabilities sufficient to support an ambitious shaping and responding strategy throughout the period covered by the Review. The RBA includes: reducing overhead and streamlining infrastructure; taking maximum advantage of acquisition reform; outsourcing and privatizing a wide range of support activities when the necessary competitive conditions exist; leveraging commercial technology, dual-use technology, and open systems; reducing unneeded standards and specifications; utilizing integrated process and product development; and increasing cooperative development programs with allies. Measures such as these can shorten cycle times, particularly for the procurement of mature systems; enhance program stability; increase efficiencies; and assure management focus on core competencies, while freeing resources for investment in high-priority areas.…

- **Insurance Policies.** The fourth element of preparing is taking prudent steps today to position ourselves to respond more effectively to unlikely, but significant, future threats, such as early emergence of a regional great power or a “wild card” scenario. Such steps provide a hedge against the possibility that unanticipated threats will emerge. The Department should focus these efforts on threats that, although unlikely, would have highly negative consequences that would be very expensive to counter.…

Military Capabilities Required to Support the Strategy

As previously noted, perhaps the greatest challenge for U.S. forces in this planning period is to maintain the near-term capabilities required to carry out the shape and respond elements of the strategy while simultaneously undergoing the transformation required to prepare now for the future. This means maintaining the ability to conduct the full spectrum of military operations required to protect and promote U.S. interests in the near term even as our military forces evolve to incorporate the new technologies, doctrine, operational concepts, training approaches, and organizational structures that will enable them to meet the challenges of 2015 and beyond.…

Critical Enablers

Critical to power projection and to our unique ability to both shape the international security environment and respond to the full spectrum of crises are a host of capabilities and assets that enable the worldwide application of U.S. military power. These critical enablers include:

- Quality people, superbly led by commanders, are our most critical asset.…

- We must have a globally vigilant intelligence system to provide early strategic warning of crises and detect threats in an environment complicated by more actors and more sophisticated technology. It must cope with increased methods of deception, rapidly changing technology, and respond to the need for shorter decision cycles.… The expanding technical ability to deliver large quantities of information selectively to tactical commanders has enormous promise and is a key element of the RMA.

- Our global communications must allow for the timely exchange of information, data, decisions, and orders, while negating an adversary's ability to interfere in our information operations. The ability to gather, process, and disseminate an uninterrupted flow of reliable and precise information anywhere in the world and under any conditions is a tremendous strategic and military advantage. These capabilities, when combined with the ability to protect one's own information systems and at the same time negate an adversary's, result in information superiority.
- The United States must retain superiority in space. Global intelligence collection, navigation support, meteorological forecasting, and communications rely on space-based assets.…
- Control of the seas and airspace support both the shaping and responding elements of our strategy, allowing the United States to project military power across great distances and protect our interests around the world.…

Without these critical enablers, the United States military could not execute the defense strategy described above.…

Alternative Defense Postures

…the QDR developed and evaluated several postures along a spectrum of the feasible approaches to meeting the strategy. All of these postures support our overall strategy. One alternative places greatest emphasis on shaping and responding in the near and midterm, while accepting greater risk in preparing now for an uncertain future. A second path emphasizes preparing now for the future, while accepting greater risk in shaping and responding in the near and midterm. And a third alternative path would attempt to balance risk over time by sustaining sufficiently large and capable forces to shape and respond in the near and midterm, while transforming the force to meet future challenges.…

Strategic Assessment of Alternative Paths

…To assess the defense postures associated with each path, we identified a number of specific criteria. These ranged from the ability to sustain permanently stationed forces abroad within acceptable personnel tempo levels, to the ability to achieve our campaign objectives in a major theater war, to the ability to maintain needed levels of investment in research and development as well as the procurement of new systems. A summary of the results of these assessments follows.

Shape. The defense strategy requires forces that are capable of providing substantial levels of peacetime engagement, drawing on the full range of shaping instruments including: forces permanently stationed abroad, forces rotationally deployed abroad, forces deployed temporarily for exercises, combined training, military-to-military interactions, and programs such as defense cooperation, security assistance, International Military Education and Training, and international arms cooperation. Our forces must be able to sustain such engagement within acceptable personnel tempo levels.…

The defense posture envisioned in Path 3 would provide a reasonably flexible set of near-term shaping options. This posture would allow us to sustain roughly 100,000 military personnel both in Europe and in Asia as well as current rotational deployments of naval, air, and ground forces. The needed program of exercises, training, and interaction with allies and friends could be sustained, albeit with increased stress on certain elements of the force.

Respond. The defense strategy requires that our forces be capable of responding across the full spectrum of crises—including deterring aggression and coercion in crises, conducting smaller scale contingency operations, and fighting and winning major theater wars. They must be able to do so in the face of asymmetric challenges, including the threat or use of NBC weapons, information operations, or terrorism. This means our forces must be multi-mission capable, proficient in their core warfighting competencies, and able to transition from peacetime activities and operations to deterrence to war. Once engaged in responding to large-scale regional aggression, our forces must be able to defeat the enemy’s initial attack in two theaters in close succession and then go on to achieve our overall campaign objectives.…

The defense posture envisioned in Path 3 provides adequate near-term capabilities to respond to the full range of crises and contingencies—albeit at somewhat greater risk than in Path 1. With this posture, we would need to continue to be selective in conducting smaller-scale contingency operations, especially those that have the potential to last a long time, but we would remain capable of defeating large-scale aggression in more than one region. Moreover, like Path 2, but over a slightly longer period of time, this posture exploits new capabilities and operational concepts to achieve battlefield dominance with smaller overall forces, improving our capabilities to respond.

Prepare. Finally, the defense strategy requires us to prepare now to meet the security challenges of an uncertain future. This means we must pursue a focused modernization effort, continue to exploit the Revolution in Military Affairs, and take prudent actions to ensure against the emergence of unlikely but significant future threats….

Path 3 focuses on preparing for an uncertain future, but not at the expense of meeting current challenges. Investing funding in Path 3 underwrites a measured modernization effort aimed at embracing the Revolution in Military Affairs and achieving the goals laid out in *Joint Vision 2010*, but not as quickly as Path 2. It introduces new systems and technologies at a reasonably aggressive rate, with modest room for new program starts. The goal for this path is to begin transforming the force to meet future challenges, while also shaping and responding to meet near-term challenges.

Conclusion

Based on these insights and assessments, the QDR concluded that the overall defense posture associated with Path 3 would best allow the Department to address the fundamental challenge presented by our strategy: to meet our requirements to shape and respond in the near term, while at the same time transforming U.S. combat capabilities and support structures to shape and respond in the face of future challenges. The posture described in Path 3 is not without risks, both near and longer term, but we believe we can mitigate these risks by more effectively managing the force and enhancing its capabilities.…

Forces and Manpower

The QDR force structure follows the broad outlines of Path 3. We will sustain the forces and capabilities needed to meet the demands of our strategy in the near term while at the same time beginning to transform the force for the future. The issue is not whether we will reshape our forces, but how and when.…

Force Readiness

As the 21st century approaches, the readiness of U.S. military forces to meet the full range of defense strategy demands has never been more important. Ready forces provide the flexibility needed to shape the global environment, deter potential foes and, if required, to rapidly respond to a broad spectrum of threats.… In recent years, Department of Defense policy and budget guidance has explicitly made readiness the top priority. Today’s challenge is to maintain this readiness edge while seeking efficiencies and improved operating procedures.…

Transforming U.S. Forces for the Future

The fundamental challenge for the Department of Defense is to ensure that we can effectively shape and respond throughout the 1997-2015 period. This means that even as we maintain the ready, versatile forces necessary to meet the challenges of shaping and responding in the near term, we must at the same time be transforming our forces, capabilities, and support structures to be able to shape and respond effectively in the future.

Joint Vision 2010 and the Future of Warfare

In an effort to guide this transformation, the Chairman of the Joint Chiefs of Staff developed *Joint Vision 2010*, a conceptual template for how America's armed forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint military operations. *Joint Vision 2010* embraces information superiority and the technological advances that will transform traditional warfighting via new operational concepts, organizational arrangements, and weapons systems. It guides the Department's preparations for the future through its focus on four new operational concepts—dominant maneuver, precision engagement, full-dimension protection, and focused logistics—that together aim at achieving full-spectrum dominance.

Information Superiority: Backbone of Military Innovation. The ongoing transformation of our military capabilities—the so-called Revolution in Military Affairs (RMA)—centers on developing the improved information and command and control capabilities needed to significantly enhance joint operations. With the support of an advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) common backbone, the

United States will be able to respond rapidly to any conflict; warfighters will be able to dominate any situation; and day-to-day operations will be optimized with accurate, timely, and secure information. Just as much of the non-defense world has become increasingly interconnected through the growth of internetted communications, the Department of Defense is working to provide a complementary, secure, open C4ISR network architecture.

The five principal components of our evolving C4ISR architecture for 2010 and beyond are:

- A robust multi-sensor information grid providing dominant awareness of the battlespace to our commanders and forces;
- Advanced battle-management capabilities that allow employment of our globally deployed forces faster and more flexibly than those of potential adversaries;
- An information operations capability able to penetrate, manipulate, or deny an adversary's battlespace awareness or unimpeded use of his own forces;
- A joint communications grid with adequate capacity, resilience, and network-management capabilities to support the above capabilities as well as the range of communications requirements among commanders and forces;
- An information defense system to protect our globally distributed communications and processing network from interference or exploitation by an adversary.

In warfare, the information superiority that these capabilities provide will significantly increase the speed of command, enabling forward deployed and early-entry forces to take the initiative away from numerically superior enemy forces and set the conditions for early, favorable termination of the conflict.

Dominant Maneuver. Enabling control of the battlespace through the multidimensional application of information, engagement, and mobility capabilities, dominant maneuver allows U.S. forces to position and employ widely dispersed joint air, land, sea, and space forces. Dominant maneuver will provide U.S. forces with overwhelming and asymmetric advantages to accomplish assigned operational tasks.

The dominant maneuver concept requires several enhanced capabilities. First, U.S. forces need to be lighter and more versatile. Basing logistics at sea and centralizing combat service support functions at higher tactical levels enable units to maneuver more quickly. Increasing the jointness of operations at lower tactical levels increases the forces' versatility in achieving their objectives. Second, mobility and lethality must be increased through greater reliance on netted firepower. Third, dominant maneuver requires more flexible strategic and tactical sea and air lift. Procurements of the Air Force's C-17 Globemaster, the Navy's Large Medium-Speed Roll-on/Roll-off (LMSR) ship, and the Marine Corps' MV-22 and Special Operations Force's CV-22 tiltrotor aircraft are examples of the Department's efforts to improve long- and medium-range lift….

Precision Engagement. Precision engagement enables joint forces to shape the battlespace through near real-time information on the objective or target; a common awareness of the battlespace for responsive command and control; a greater assurance of generating the desired effect against the objective or target due to more precise delivery with increased survivability for all forces, weapons, and attack platforms; and the flexibility to rapidly assess the results of the engagement and to reengage with precision when required.

Precision engagement requires more capable attack platforms and advanced weapons and munitions in addition to the enabling support of a C4ISR common backbone. The Department will be adding to its arsenal several more capable attack platforms for engaging targets on the ground and in the air, including the F/A-18E/F, F-22, and Joint Strike Fighter tactical aircraft; the Comanche and Apache Longbow helicopters; the Crusader artillery system; and the SC-21 family of new surface combatants and possibly the Maritime Fire Support Demonstrator. The Department is also developing and fielding numerous advanced weapons and munitions including improved stand-off weapons such as the Joint Air-to-Surface Standoff Attack Missile and the Joint Standoff Attack Weapon; bombs that can be accurately delivered from medium altitude, such as the Wind-Corrected Munitions Dispenser and the GPS-aided Joint Direct Attack Munition; and a new generation of anti-armor weapons such as the Brilliant Anti-Tank and Skeet submunitions.

Precision engagement is based on intelligence about enemy forces and expert judgment as to the correct force or weapon needed to generate the desired effects. The Services are working to increase the precision of infantry weapons and improve field equipment to ensure the individual soldier or Marine is fully integrated into the advanced systems that create precision engagement. Precision engagement also extends to the full spectrum of operations in which U.S. forces are likely to participate. Precise, nonlethal weapons are also currently under development for use in smaller-scale contingencies such as noncombatant evacuations and peace operations.

Full-Dimensional Protection. Protection for U.S. forces and facilities must be provided across the spectrum, from peacetime through crisis and war and at all levels of conflict. To achieve this goal, full-dimensional protection requires a joint architecture that is built upon information superiority and employs a full array of active and passive measures at multiple echelons. Full-dimensional protection will enable U.S. forces to maintain freedom of action during deployment, maneuver, and engagement....

U.S. forces also need improved protection against chemical and biological weapons threats.... Full-dimensional protection also includes defense against asymmetric attacks on information systems, infrastructure, and other critical areas potentially vulnerable to non-traditional means of interdiction or disruption.

Focused Logistics. Focused logistics integrates information superiority and technological innovations to develop state-of-the-art logistics practices and doctrine. This will permit us to accurately track and shift assets, even while en route, thus facilitating the delivery of tailored logistics packages and more timely force sustainment at the strategic, operational, and tactical level of operations. Focused logistics will reduce the overall size of logistics support while helping to provide more agile, leaner combat forces that can be rapidly deployed and sustained around the globe.

Initiatives such as Joint Total Asset Visibility and the Global Combat Support System will provide deployable, automated supply and maintenance information systems for leaner, more responsive logistics. These programs, as well as a host of Service initiatives—such as the Marine Corps' Asset Tracking Logistics and Supply System—will be capable of supporting rapid unit deployment and employment and will better support the battlefield commander by eliminating redundant requisitions and reducing delays in the shipment of essential supplies....

Conceptual Approaches To Exploit The Revolution In Military Affairs

The goals set forth in *Joint Vision 2010* are the foundation for a broader effort to exploit the Revolution in Military Affairs. Indeed, the U.S. military is committed to realizing joint and Service visions of modern warfare and is taking a number of steps to do so, including studies, wargames, R&D, advanced concept technology demonstrations, and simulated warfighting experiments. Through these efforts, which are being pursued vigorously in each Service, the armed forces are identifying, developing, and testing concepts and capabilities that will ensure their ability to transform for the future.

Army. The Force XXI and The Army After Next processes are identifying new concepts of land warfare that have radical implications for the Army's organization, structure, operations, and support.

Lighter, more durable equipment will enhance deployability and sustainability, and advanced information technologies will help the Army conduct decisive operations. The force will be protected by advanced but easy-to-use sensors, processors, and warfighting systems to ensure freedom of strategic and operational maneuver….

The Army sustains separate, but complementary, efforts in a continuous process to implement the visions identified in Force XXI and The Army After Next. Current efforts are aimed at enabling today's soldiers and combat systems with information technology and other enhancements while beginning long-term research and development efforts. The Army's Experimental Force (EXFOR) is the vehicle for testing these innovations. EXFOR is a digitized heavy force used to identify and evaluate new operational concepts, organizational designs, advanced technologies, doctrine, and tactics through the Army's Advanced Warfighting Experiments. The Army After Next program is a comprehensive initiative designed to better understand the probable nature of warfare 30 years into the future and provide focus to today's development efforts….

Air Force. Global Engagement: A Vision for the 21st Century Air Force, the Air Force's vision of air and space warfare through 2010, calls for maintaining and improving six core competencies built on a foundation of quality personnel and integrated by global battlespace awareness and advanced command and control. Air and space superiority will allow all U.S. forces freedom from attack and freedom to attack, while the Air Force's ability to attack rapidly anywhere on the globe will continue to be critical. Rapid global mobility will help ensure the United States can respond quickly and decisively to unexpected challenges to its interests. The Air Force's precision engagement core competency will enable it to reliably apply selective force against specific targets simultaneously to achieve desired effects with minimal risk and collateral damage. Air- and space-based assets will contribute to U.S. forces' information superiority, and agile combat support will allow combat commanders to improve the responsiveness, deployability, and sustainability of their forces....

Navy. The Navy's future vision of warfare, delineated in *From the Sea* and *Forward…From the Sea*, and further developed in the Navy Operational Concept, identifies five fundamental and enduring roles: sea control and maritime supremacy, power projection from sea to land, strategic deterrence, strategic sealift, and forward naval presence. However, in the future the Navy will fulfill these roles with vastly enhanced capabilities. The Navy has embraced an RMA concept called Network-centric Warfare: the ability of widely dispersed but robustly networked sensors, command centers, and forces to have significantly enhanced massed effects. Combining forward presence with network-centric combat power, the Navy will close timelines, decisively alter initial conditions, and seek to head off undesired events before they start. The naval contribution to dominant maneuver will use the sea to gain advantage over the enemy, while naval precision engagements will use sensors, information systems, precisely targeted weapons, and agile, lethal forces to attack key targets. Naval full-dimensional protection will address the full spectrum of threats, providing information superiority, air and maritime superiority, theater air and missile defense, and delivery of naval fires. Finally, naval forces will be increasingly called upon to provide sea-based focused logistics for joint operations in the littorals.…

Marine Corps. Marine Corps *Operational Maneuver from the Sea* foresees warfare that requires tactically adaptive, technologically agile, opportunistic, and exploitative forces. Individuals and forces must be able to rapidly reorganize and reorient across a broad range of new tasks and missions in fluid operational environments. The Marines will still need to project power ashore for a variety of potential tasks ranging from disaster relief to high-intensity combat.

The focus of Marine Corps RMA efforts is on the enhancement of the individual Marine and his or her ability to win in combat. The Marine Corps Combat Development System focuses on generating the most effective combination of innovative operational concepts, new organizational structures, and emerging technologies.…

Exploration of the RMA in the Long Term

By conducting several research efforts that look out to 2020 and beyond, the Department seeks to ensure it will be prepared for a range of plausible futures. The Army's Dominating Maneuver wargames and workshops explore operational concepts and RMA force characteristics that might be relevant in the 30-year time frame. The Air Force is now planning its transition from an air and space force to a space and air force through the Chief of Staff's institutionalized long-range planning process, which has identified new operational concepts and the paths to implement those concepts. The Chief of Naval Operations' Strategic Studies Group likewise has concept generation teams that are investigating future naval warfare concepts, from rotational base issues to asymmetric capabilities and responses. In addition, the Marine Corps' Operational Concepts wargames and New Science projects are examining nonlethal and other innovative technologies, as well as the application of algorithms from other disciplines, such as the natural sciences, to military art and science.

OSD's Office of Net Assessment has also developed an Operational Concepts Wargaming Program with support from the Services. This program will explore concepts such as dominant maneuver, Air Force modernization concept alternatives, "future Navy," space war, and information warfare. The Department's science and technology (S&T) efforts are directly linked to *Joint Vision 2010* concepts and are guided by concept-related Defense Technology Objectives (DTOs). Each DTO identifies a specific future technology advancement that will be developed or demonstrated, the anticipated date of technology availability, and the benefits likely to result from the technology advance....

Additionally, the Defense Advanced Research Projects Agency is investigating a satellite constellation, know as "Starlite," that can provide on-demand radar imagery anywhere and in near real-time to the theater commander, and a "Situational Awareness System" that will link the Internet to the warfighter via an arm-mounted terminal....

QDR Modernization Decisions: Supporting the Transformation of U.S. Forces

The Department's extensive modernization effort, which will reach the aggregate procurement spending objective of $60 billion per year shortly after the turn of the century, directly supports efforts to realize the modern, joint capabilities called for by *Joint Vision 2010* and to exploit the RMA in accordance with the "prepare now" tenet of our defense strategy. The QDR modernization review focused on a number of programs for evaluation and decision, in order to ensure that future U.S. forces have modern, technologically superior equipment, that systems are effectively integrated across platforms and Services, and that programmatic and operational risks were weighed in the context of force requirements. Several of these decisions resulted in programmatic changes, highlighted below.

C4ISR. Because modernization of our forces depends on a strong C4ISR common backbone and because these systems require significant resources, the Department undertook a hard and sweeping look at our entire C4ISR effort. While a number of programmatic adjustments were evaluated, we did not change the general focus and amount of resources devoted to C4ISR in the QDR. The net effect of the programmed investments will be to substantially improve our awareness of various types of enemy forces in the areas adjacent to our forces and at longer ranges as well. We will continue to evolve toward more interoperable battle management systems with the initial deployment of the Global Command and Control System (GCCS) below the joint command level and into operational Service units. The Department is committed to achieving information superiority and to the resolution of remaining challenges over the next several years. A significant C4ISR challenge is to overcome deficiencies in our ability to move information in a timely manner to the lowest tactical levels. We will fund efforts to meet such challenges by correcting certain imbalances in the overall C4ISR program and by more aggressively using advanced technologies to reduce ongoing program costs. Decisions on C4ISR will be made in the context of other decisions on force structure, force design, weapons platforms, munitions, and information-enabled operational concepts.

JSTARS. The Joint Surveillance and Target Attack Radar System (JSTARS) provides radar data on fixed and moving targets from an airborne battle management platform that enhances our combat forces' ability to operate throughout the battlespace in responding to crises. In conflict, the JSTARS tracking data can be used by on-board and ground-based controllers to help direct timely attacks on a wide range of targets. Our approach to system development provides important enhancements to the U.S. JSTARS fleet and reflects our commitment to support NATO's consideration of the Alliance Ground Surveillance (AGS) capability.

The Department has decided to reduce the overall U.S. JSTARS fleet from 19 to 13 aircraft. A fleet of this size will provide round-the-clock coverage needed in a major theater war. Some portion of these aircraft would have to be redeployed in the event of a second major theater war.…

We will also explore the potential for supplementing radar coverage of enemy force movements from long-endurance unmanned aerial vehicles (UAVs). In addition, our approach provides funds for key upgrades to U.S. JSTARS, including radar upgrades and improved connectivity to weapon platforms and broadcast intelligence.

Tactical Aircraft. Our review of tactical aircraft programs focused on the F-22 Raptor, the F/A-18 E/F Super Hornet, and the Joint Strike Fighter (JSF). We assessed alternatives to these programs from the standpoint of both warfighting risk and acquisition cost. Termination of any of the three fighter programs was not considered prudent given the warfighting risk of such a decision and the significant adverse impact it would have on technology development and the defense industrial base.…

Deep Strike/Anti-Armor Weapons and Munitions. In the wake of the Deep Attack Weapons Mix Study, the Department determined that the current munitions programs, with modest adjustments, will provide the capability to defeat potential aggressors in the years ahead. The next generation of munitions will give our forces superior precision engagement capability against projected threats.…

For the “deep battle,” the following systems will be procured in accordance with existing plans: the Wind-Corrected Munitions Dispenser carrying Combined Effects Bomblets or the “brilliant” Skeet anti-armor submunition; the Army Tactical Missile System with Brilliant Anti-Armor Submunitions (ATACMS BAT/BAT Pre-Planned Product Improvement); the product improved version of the Sensor-

Fuzed Weapon, and the Joint Stand-Off Weapon (JSOW) with a unitary warhead.…

Ship Modernization. The Navy's ship modernization program will ensure the United States retains the ability to control the seas and project power ashore in peacetime and across the broad spectrum of contingencies.…

Army Ground Combat. The Army faces both near- and long-term challenges in executing its currently planned modernization program. Reductions in operations and support costs will help us achieve needed modernization funding increases and will provide some additional resources above those previously planned. These additional resources will address a number of the Army's most pressing modernization needs. For example, the Army will accelerate the fielding of a digitized (Force XXI) corps and complete Army National Guard Division Redesign more quickly.

"Digitization" involves the use of modern communications capabilities and computers to enable commanders, planners, and shooters to rapidly acquire and share information. This improved awareness will revolutionize the conduct and tempo of all phases of combat operations. The results of recent Army Warfighting Experiments at Fort Irwin and follow-on experiments will be used to determine the force structure, materiel requirements, and doctrine for digitized units. The Army had planned to field the first digitized corps in 2006. This corps now can be fielded one to two years sooner.…

Navigation. Upgrades to the space-based Global Positioning System (GPS) and compliance with Global

Air Traffic Management (GATM) rules that will be coming into force over the next several years will require significant future expenditures which are yet to be determined. The navigation challenge is to efficiently implement upgrades to the GPS satellite constellation and user navigation equipment that allows us to respond effectively in time of crisis and to facilitate our participation in the GATM system and other navigation and safety efforts….

Transforming Our Response to Asymmetric Challenges

Integral to our efforts to transform the Department for the future are our efforts to address a range of asymmetric challenges. Measures to prepare our forces to face these challenges, from fielding new capabilities to adapting how U.S. forces will operate in future contingencies, are already underway. To ensure that U.S. forces will be able to respond effectively to such challenges through the year 2010 and beyond, the Office of the Secretary of Defense, the Joint Staff, the Services, and the CINCs are working together in several areas. Chief among these are threats of NBC weapons use, terrorism, and information warfare.

Counterproliferation. In recent years, the Department has made substantial progress toward fully integrating the risks associated with an adversary's NBC weapons use into our military planning, acquisition, intelligence, and international cooperation activities. This need was underscored in the major theater war assessment done in the QDR. Accordingly, the Secretary of Defense has increased planned spending on counterproliferation by approximately $1 billion over the program period, particularly for protective measures against chemical weapons. With this additional investment, the Department will continue to strengthen existing U.S. capabilities.…

Force Protection and Combating Terrorism. Over the past few years, and particularly following the attack on Khobar Towers, the Department has moved swiftly to reduce American vulnerability to terrorist attacks and to make U.S. forces as preeminent in combating terrorism as they are in other forces of warfare. The Department will ensure that U.S. forces operate under mandated standards for combating terrorism, improve intelligence collection, distribution, and information-sharing with allies, and strengthen our capability to protect citizens and military personnel from chemical or biological attacks with special emphasis on high threat regions.…

Information Operations. Efforts to exploit information technology to adapt and transform the U.S. military are well underway. To date, the Department has directed most of its efforts in this area toward protecting critical U.S. infrastructure against hostile information operations and developing U.S. information operation capabilities for use in peacetime engagement activities, smaller-scale contingencies, and major theater wars.

Although our current capabilities are adequate to defend against existing information operations threats, the increasing availability and decreasing costs of sophisticated technology to potential adversaries demand a robust commitment to improve our ability to operate in the face of information threats as we approach the 21st century. Critical to ensuring that ability will be the institutionalization of information operations—that is, the integration of information operations concepts into military planning, programming, budgeting, and operations. In the context of *Joint Vision 2010*, we will continue to develop additional guidance to strengthen information assurance—the protection, integrity, and availability of critical information systems and networks. Further, we will allocate adequate resources for these efforts within our information technology investment programs and improve the Defense-wide planning and implementation process, regularly assessing funding adequacies for all information assurance program components.

Defense against hostile information operations will require unprecedented cooperation between the Department of Defense, other federal agencies, the armed forces, commercial enterprises, our allies, and the public. The Department is working closely with the Presidential Commission on Critical Infrastructure to develop this cooperative relationship. Technical measures to protect military information systems, both hardware and software, are being greatly expanded, and all Services now provide capabilities to test and assess their information networks and systems. Capabilities to protect information systems must also extend beyond traditional military structures into areas of civilian infrastructure that support national security requirements, such as the telecommunication and air traffic control systems.

Offensive actions to disrupt our adversary's access to information are also part of U.S. military capabilities. Such capabilities will be increased in the future to ensure that the United States maintains information superiority during a conflict.

Conclusion

Preparing now for future challenges is critical to the success of our defense strategy throughout the 1997-2015 time frame. The Department is committed to implementing and underwriting *Joint Vision 2010* and complementary Service visions. Efforts to modernize our current force are integral to that implementation; even more important are efforts to leverage new technologies to harness the Revolution in Military Affairs through new operational concepts, new doctrine, and, ultimately, organizational changes. In addition, the Department must institutionalize innovative investigations, such as the battle laboratories and warfighting experiments, to ensure future concepts and capabilities are successfully integrated into the force in a timely manner. Finally, we must remain ever vigilant against asymmetric strategies that threaten our forces and citizens by strengthening efforts to reduce their likely use and potential impact and by developing a range of response options. Through all of these efforts and activities, DoD is transforming itself at a substantial pace.

Achieving a 21st Century Defense Infrastructure

Our military forces and operations are changing dramatically in response to the changing security environment and advances in technology. The way we support the warfighter must also change. The Department must be leaner, more efficient, and more cost effective in order to serve the warfighter faster, better, and cheaper. We not only have the opportunity to change, we have the requirement to change. The forces envisioned in *Joint Vision 2010* will require a radically different support structure. Achieving those forces will also require steadily increasing investments. To afford these investments, the Department will need to achieve offsetting efficiencies in support operations.…

To close the gap between force structure and infrastructure reductions and begin to reduce the share of the defense budget devoted to infrastructure, the QDR is proposing the following four actions:

- Make a further reduction of 109,000 civilian personnel associated with infrastructure beyond the initiatives in the DoD budget for FY 1998.…
- Request authority for two additional rounds of BRAC, one in 1999 and the second in 2001.
- Improve the efficiency and performance of DoD support activities by adopting innovative management and business practices of the private sector. These include “reengineering” or “reinventing” DoD support functions, e.g., streamlining, reorganizing, downsizing, consolidating, computerizing, and commercializing operations.

As a critical part of this reengineering, consider far more non-warfighting DoD support functions as candidates for outsourcing.…

Defense Resources

The QDR included considerations of the fiscal environment in developing a program to meet the requirements of the defense strategy. Absent a marked deterioration in world events, the nation is unlikely to support significantly greater resources dedicated to national defense than it does now—about $250 billion in constant 1997 dollars per year….

Fulfilling a strategy of shaping the international security environment, responding to the full spectrum of crises and aggression, and preparing now for the future require substantial and ready forces, together with a focused program of investments to improve the equipment those forces will employ. Although existing plans continue to project significantly increased funds for modernization, the Department's record of having to pay operating expenses out of funding planned for investment threatens the viability of those plans. Therefore a focus of the QDR was to build a solid financial foundation for a modernization program that could reliably support the future warfighting capabilities called for by *Joint Vision 2010*. The key to that foundation is to halt the chronic disruption to modernization plans by properly projecting and funding the Department's operating and support activities….

The Modernization Imperative

In the years immediately following the end of the Cold War, the Department's reduction in spending came disproportionately from reductions in procurement spending, a decision that reflected a prudent, calculated risk initiated by the administration of President Bush and continued by this administration. This approach was possible because large quantities of modern equipment had been purchased during the 1980s and force reductions had permitted the retirement of older ships, aircraft, and armored vehicles in the early 1990s. That drawdown is now over, the dividend from procurement reductions has been spent, the procurement holiday must end, and investment in modernization needs to rebound. Otherwise, the technological superiority of our forces—and our ability to sustain their equipment stocks—will erode over time.

However, each new defense program since completion of the Bottom-Up Review in 1993 had had to postpone the previous year's plan to begin increasing procurement spending.…

These postponements have been a reflection generally of the high priority the Department attaches to current spending on readiness. But in addition, they have occurred because our planning has not managed financial risk in a way that reflected the importance we also attach to investing in the future.…

Assessing Resource Challenges

Consequently, a principal resource management objective of the QDR has been understanding financial risk in the Department's program plans and devising approaches to manage that risk.… The assessment focused on three sources of disruption to the Department's program plans:

Migration. The primary source of instability in the Department's current plans is the migration to other activities of funding planned for procurement. This chronic erosion of procurement funding has three general sources:

- Unprogrammed operating expenses.…
- Unrealized savings.…

- New program demands.…

Long-Term Challenges. The first long-term challenge to the defense program is represented by potential shortfalls in minor procurement funding.…

A second long-term resource challenge concerns projections of funding requirements for modernization beyond the end of the current program in 2003. As successive FYDPs reduced the amount of procurement programmed in the 6-year planning period, some of these reductions have accumulated into long-term projections, creating a so-called “bow wave” of demand for procurement funding in the middle of the next decade.…

Technical Risk and Uncertainty. Complex technologically advanced programs all bear some risk of costing more than planned. When unforeseeable growth in costs occurs, offsets from other programs must be found, which in turn disrupts the overall modernization program. Our programming process must provide sufficient flexibility in the form of program reserves to address this risk. As a result of the QDR analysis, each military department plans to establish a prudent funding reserve in its out-year plans to offset these types of cost increases and significantly reduce one of the destabilizing factors affecting our modernization programs. Additionally, the Department will select several “pilot programs” that will carry similar reserves in the budget as a means of mitigating significant cost or schedule impacts that arise in the year of execution.…

Comments by the Chairman of the Joint Chiefs of Staff

…Today we are presented with a unique strategic opportunity. For more than 50 years we were constrained by a bipolar rivalry with a superpower adversary. To deal with such a world, we relied on a strategy of containment and designed our military forces to react in case the strategy failed. Today and tomorrow, we have an opportunity to pursue a strategy of engagement and to design a military force to help the strategy succeed.

I fully agree with the defense strategy of helping to shape the environment to promote U.S. interests abroad; of being prepared to respond with ready forces to crises from smaller-scale contingency operations to major theater wars; and of preparing for an uncertain future.…

Our challenge is to balance risk between near-term requirements and the need to prepare for the longer term. We must dominate the future battlefield, where technology will change the face of warfare, as we dominate it today. We must start now to prepare for a potentially more dangerous future which promises continuing risks and challenges, including asymmetric threats such as terrorism, chemical and biological weapons, and information warfare.…

The Future

…The future offers us great opportunities. Warfare is changing with the growth of technological change, and we must not only stay abreast of it, but dominate it. Remarkable advances in information technology, stealth, and precision strike promise a real revolution in military affairs. But implementing the RMA will require a sustained effort, a process of balances evolution toward revolutionary capabilities. *Joint Vision 2010* provides a prudent vector for combining revolutionary technological advances with new operational concepts to give us a force to dominate any future battlefield….

PART THREE

INTRODUCTION

Not surprisingly, U.S. Department of Defense positions on Information Age warfare have generated both believers and skeptics. This section provides analyses and discussion from two of each.

The first article, excerpts from Jeffrey R. Barnett's *Future War: An Assessment of Aerospace Campaigns in 2010*, wholeheartedly accepts information-related technologies as the key to future warfare. Barnett states his position simply, "Information will dominate future war. Wars will be won by the side that enjoys and can exploit: cheap information…accurate information…near-real-time information…and pertinent information."

Barnett identifies six areas in which warfare that focuses on information will mirror traditional war. IW will have offensive and defensive dimensions. It will be conducted at strategic, operational, and tactical levels. It will both support other military campaigns and operate independently. IW will be an imperative for victory. Military forces must be able to operate despite successful enemy IW operations. And IW will have distinct mission types. Nevertheless, Barnett sagely cautions, even with IW's great and growing importance, there will be a tendency to overstate its importance.

Barnett next introduces the concept of parallel war, that is, near-simultaneous operations against an enemy at all levels and across all target categories. Although the idea of parallel war is not new, Barnett maintains that in the past, military capabilities were not sufficient to allow it to be accomplished. He asserts that now, however, advances in four key Information Age technologies—information availability, command and control, penetration, and precision—will permit it to be achieved. Concentrating on aerospace warfare, Barnett then applies these concepts to scenarios that place the U.S. at war first with a peer competitor and next with a niche competitor (called by others regional powers).

Although he emphasizes that "the chance of war with a peer is remote," he also stresses that "times change." If and when a peer competitor emerges, Barnett believes that both sides will have atmospheric and space-based reconnaissance and information systems, integrated and redundant command and control systems, stealth aircraft and cruise missiles, and precision weapons. The presence of such capabilities in an enemy's arsenal will present challenges to U.S. military planners far beyond those that are presented today by any likely enemy. He stresses that while the technologies are important, "superior employment concepts" must also be developed.

Barnett identifies eleven different operational concepts critical to aerospace operations in a future war against a peer, one of which is supporting the information campaign. To Barnett, aerospace forces should expect heavy tasking in such a campaign. They should also expect to be under information attacks in which the enemy attempts to degrade the U.S. ability to collect information and to corrupt information that is collected.

Barnett also stresses that Information Age technologies push decision-makers toward near-real-time decisions. Here, Barnett sees a risk as automation and threat/opportunity triggers are increasingly used. He also notes the importance of understanding an enemy's decision cycle and being able to corrupt that cycle, thereby forcing the enemy to make slower decisions as he checks his data and decision processes. Barnett concludes his discussion of war with a peer competitor by offering eighteen aspects of conflict that he believes merit special consideration.

In his discussion of war with a niche competitor, Barnett begins by identifying "five key points to remember." First, a niche competitor will "always be militarily inferior to the U.S." Second, the niche competitor will have vulnerable operational centers of gravity. Third, many states could obtain niche status, but all will have "operational proficiency in only a few mission areas." Fourth, niche competitors must be expected to employ and control new technologies in innovative ways. Finally, war with a niche competitor will be a "come as you are" war that will probably preclude threats to vital U.S. interests.

From these five key points, Barnett then builds a scenario in which a niche competitor has great capabilities in some areas and limited capabilities in other areas and uses "asymmetric employment schemes" such as degrading U.S. information flows and complicating U.S. force projection efforts. Conversely, Barnett says, the U.S. should concentrate on operational concepts against a niche competitor such as paralyzing command and control, dominating battlefield awareness, integrating information obtained from space-based and unmanned aerial surveillance systems, supporting the general information campaign, and attacking enemy wealth and its ability to generate it.

Barnett concludes by identifying a set of “near-term actions that he believes are mandatory to prepare for conflict against either a peer or a niche competitor. These include designating a focal point for future warfare and building both a concept development center and an information warfare center. (Some of these steps have been undertaken since Barnett’s work was published.) He also believes the U.S. should task the Defense Intelligence Agency for comprehensive future projections, study out-of-theater command and control, study centralized control of national and theater collection platforms, organize for information warfare, and organize for parallel war.

Some of these suggestions, of course, are easier said than done. And in all cases, as we move toward a future made uncertain by emerging Information Age technologies, the devil of implementation will be in the details. Nevertheless, Barnett clearly believes that Information Age technologies are significantly altering and will further alter the ways in which wars are fought.

Arthur K. Cebrowski and John J. Garstka, authors of the next chapter, “Network-Centric Warfare: Its Origins and Future,” share that belief. Concentrating on naval warfare and the U.S. Navy, Cebrowski and Garstka begin their analysis by arguing that changes in economics, information technology, and business processes and organizations are fundamentally changing U.S. society, and that these changes in turn demand and force changes in military affairs. The authors link these changes via three themes:

1. a shift from platforms to networks;
2. a shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem; and
3. the importance of making strategic choices to adapt and survive.

Positing that "nations make war the same way they make wealth," Cebrowski and Garstka see advances in information technology (IT) as the central feature in changing the economic structure of the world, let alone individual states. IT itself is changing, they also observe, moving from a platform-centric computing environment to a network-centric environment. These changes in turn have been adapted by American business as more and more firms focus on IT and network-centric operations. This strengthens the businesses that make these changes, and so too, the authors assert, it should be with the American military. It must adopt the concept of "network-centric warfare."

Strategically, this means that the U.S. military must acquire a "detailed understanding of the appropriate competitive space," elsewhere termed dominant battlespace knowledge. Operationally, this means that all units must be closely linked both to each other and to the operating environment. Tactically, "speed is critical." Structurally, the authors point to a need for an operational architecture that includes sensor and engagement grids, a high-quality information backplane, and value-added command processes much of which must be automated.

Together, these features will allow U.S. forces to act more rapidly than enemy forces. This "speed of command," as the authors terms it, will enable U.S. forces to "lock-out" enemy options, disrupt enemy strategy, and maintain combat initiative. They will also allow U.S. forces to "self-synchronize," that is, to organize themselves from the bottom up to meet the commander's intent. Time between decisions and actions shorten, thereby allowing more rapid action and again denying the enemy options.

All this, the authors maintain, is beginning to happen now, especially in the Navy. Nevertheless, Cebrowski and Gartska say, more change is needed, especially in three areas, intellectual capital, financial capital, and process. The authors then detail why these areas are important and why more change in each area is needed. While they believe the future is bright vis-à-vis the military's willingness and ability to initiate and implement requisite change, they nevertheless conclude with a cautionary note from B.H. Liddell Hart: "The only thing harder than getting a new idea into the military mind is getting an old one out."

The authors of the next two articles in this section would probably disagree with Liddell Hart, at least as regards getting new ideas into the military mind. Thomas P.M. Barnett in "The Seven Deadly Sins of Network-Centric Warfare" and William Hoehn in "What Revolution in Military Affairs?" are concerned that many in the U.S. military have too fully adopted the precepts and beliefs of network-centric warfare and the revolution in military affairs without sufficient attention to the flaws that may exist in both.

Without completing rejecting the concept (they are “deadly sins,” he says, not “mortal sins”), Thomas Barnett takes network-centric warfare to task in seven specific area. His first perceived “deadly sin” is the fact that no one except the United States is truly experiencing a revolution in military affairs. Pointing out that the U.S. military annually spends more on its information technology than all but a few countries spend on their entire defense establishments, Barnett concludes that network-centric warfare (NCW) “longs for an enemy worthy of its technological prowess.”

Barnett next observes that NCW prepares the U.S. for the type of war that it is least likely to fight, large-scale conflict, even as it slows the adaptation of U.S. military forces to capabilities appropriate for the type of conflict they are most likely to experience, military operations other than war (MOOTW). In a world rife with MOOTW, Barnett asks, should the United States not be more concerned with wiring itself to the outside world so it can cope better with MOOTW rather than wiring up its military internally?

Barnett’s third perceived deadly sin is his belief that as implemented by the U.S. Navy, network-centric warfare leads to the development of more and more costly platforms, fewer and fewer of which can be procured because of their cost. This, Barnett says, flies in the face of a true network-centric system in which no node of the network is “worth more than the connectivity it provides.”

Fourth, to Barnett, arguments that NCW and information dominance will lock an enemy out of certain courses of action and force him into others “resurrect old myths” about swift “bloodless victory.” This, to Barnett, is simply wrong. Positing that “one man’s information warfare is another man’s international terrorism,” Barnett asserts that the U.S. lacks “the decision assessment tools at this point to steer an opponent via information dominance.”

The author next raises the question whether network-centric warfare’s emphasis on “getting inside the enemy’s decision loop” could push the U.S. into “shooting first and asking questions later.” Speed of decision, Barnett cautions, should not be the objective, but rather “how best to exploit the delta between our loop time and his.”

Sixth, Barnett questions network-centric warfare’s emphasis on self-synchronization. As with the preceding “deadly sin,” Barnett maintains that NCW’s emphasis on speed of action from decentralized sites could lead the American military to “de-emphasize the rational thinking that must periodically interrupt whatever courses of action our commanders in the field are empowered to pursue.” This, Barnett warns, would be dangerous.

Finally, Barnett fears that NCW’s emphasis on developing a “common operating picture” for “all players at all levels” could lead to “information overload” in which the common operating picture is “neither shared nor real.” Unlimited data flow to all levels, Barnett asserts, “may prove more disintegrating than integrating.”

Despite these criticisms of NCW, Barnett in his conclusion professes his belief that a networking paradigm for future conflict is inevitable. He argues strongly, however, that such networks should be "focused outwardly" rather than inwardly, and that they must reach out to sub-national environments "below the level of the nation-state" rather than concentrating on "large-scale violence."

In "What Revolution in Military Affairs?," William Hoehn is even more critical of the direction of modern U.S. military thought. Whereas Barnett restricts his criticism to NCW and ends on a favorable note, Hoehn takes on the entire concept of the revolution in military affairs and concludes that the RMA's vision of "a perfect war capability"—what Hoehn describes as "the perfectionist application of precisely measured forces to defeat an enemy rapidly, thoroughly, and completely, with no U.S. troops at risk and no U.S. casualties"—is not possible now and will not be possible far into the future.

Hoehn reached these conclusions on the basis of several elements of evidence. Noting the RMA is predicated on "the seamless melding of technologies in three areas: intelligence, surveillance, and reconnaissance; command, control, communications, computers, and information dissemination; and precision force," the author identifies several obstacles that may frustrate the seamless melding the RMA requires. These include the technological unfeasibility of several required surveillance and reconnaissance elements, the integration of all elements into a well-functioning system-of-systems, and insufficient "Red Teaming" of the RMA concept.

Hoehn then identifies several possible counters to the RMA that an enemy may employ. Examining first "momentary interruptions," the author argues that stealth technology could well degrade the capabilities required for the RMA, as could any other momentary disruption of the "complex and highly interactive" data flow needed for the RMA to work. Hoehn also ponders whether an enemy might use methods such as a high altitude nuclear explosion to generate an electromagnetic pulse to render U.S. connectivity inoperative and to degrade operational capabilities of U.S. forces.

Hoehn also raises questions about how much added value the RMA actually brings to large-scale maneuver warfare, to "hostage scenarios" in which an enemy captures or threatens to capture a territory of great value, and to asymmetric warfare ranging from guerrilla and urban warfare to terrorism and information warfare. In all areas, Hoehn finds the reality and promise of the RMA wanting.

Together, then, the believers and skeptics paint a mottled picture of what the reality is and the hope may be for the application of Information Age technologies to modern military affairs. Given the plans of the Pentagon, the hopes of the believers, and the doubts of the skeptics, it is little wonder that debate rages on about the future of warfare in the Information Age.

CHAPTER 13

FUTURE WAR:

AN ASSESSMENT OF AEROSPACE CAMPAIGNS IN 2010

(excerpts)

By
Jeffrey R. Barnett

Overarching Concepts

As we look to the future, the growth of information technologies seems limitless. Hardly a day goes by without a breakthrough of some kind in information-related technologies. For this reason, it is likely both the United States and an enemy will have information-based systems far more advanced than those currently available. Both the United States and its enemy could have:

- global satellite networks with voice, data, and imaging capabilities 50 times greater than today (based on advances in data compression, processing, frequency management, miniaturization, and sensors). Although the military will control a limited number, commercial interests will own most platforms.

- autonomous weapons, enabled by artificial intelligence, automatic target recognition algorithms, and multispectral miniature sensors.

- sophisticated computer viruses—and equally sophisticated encryption protocols.
- data fusion at rates 104 times faster and more accurate than today, based on advances in processing and software.[1]
- data storage capabilities at 103 times greater than today (due to miniaturization).

Information War

Because of these and other advances, an information campaign will be integral to any future conflict. Simply stated, information will dominate future war. Wars will be won by the side that enjoys and can exploit: cheap information while making information expensive for its opponent; accurate information within its own organization while providing or inserting inaccurate data in its opponent's system;[2] near-real-time information while delaying its opponent's information loop; massive amounts of data while restricting data available to its opponent; and pertinent information while filtering out unnecessary data.

The United States does not have a monopoly on this insight. The impact of information technologies on war is well understood abroad. According to one Chinese defense intellectual: "(I)n hi-tech warfare, tactical effectiveness no longer depends on the size of forces or the extent of firepower and motorized forces…."[3]

Military theorists in Russia hold a similar view. Major General Vladimir I. Slipchenko (Retired), the leading Russian military theoretician, (declares): "The impending sixth generation of warfare, with its centerpiece of superior data-processing to support precision smart weaponry, will radically change military capabilities and, once again, radically change the character of warfare."[4]

Military professionals should feel comfortable envisioning campaigns focused on information. Although an information focus brings new targets and weapons to war, it nevertheless mirrors traditional military concepts in at least six general ways.

1. As with all forms of warfare, information war (IW) will have offensive and defensive aspects. Militaries will both prosecute information war and defend against its use by the enemy.

2. Information war will be conducted at the strategic, operational, and tactical levels of war. Decision makers at each level will orchestrate information campaigns. They'll attack information infrastructures at the national, theater, and unit levels.

3. Information war will both support other military campaigns and operate independently. For example, just as naval air forces have both independent (e.g., antisubmarine warfare) and supporting (e.g., close air support) missions, information components will sometimes support other operations and sometimes require the support of other forces.

4. Information war will be an imperative for victory. Even as past victories were possible only through supremacy of the air, land, or sea, future victories will be doubtful without information supremacy.

5. Military forces must be capable of operations despite successful enemy IW. Because perfect defenses against IW are an unreasonable expectation, units must continue functioning despite corrupted information.

6. Information war will have distinct mission types. As with conventional military forces, no one type of IW will suffice to describe all its ramifications. For example, just as aerospace power has distinct mission types (e.g., airlift, interdiction, counterair), IW will have subsets.…

Given the critical importance of information to future war, the theater commander should have a component commander dedicated solely to winning the information campaign. Other components will have tactical information forces and interests to be sure, but to orchestrate information war at the strategic and operational levels, both offensively and defensively, the CINC should designate one commander and organization responsible for fighting and winning the information campaign.[5] This will be a critical campaign. Army Secretary Michael P. W. Stone reported after the 1991 Gulf War:

> *The first priority of coalition forces during the offensive phase was the systematic destruction of Iraqi Command, Control, and Communications (C3). The same offensive strategy is likely to be employed against U.S forces by any future adversary.*[6]

The joint force information component commander (JFICC) should have five goals:

1. Collect information on enemy capabilities, deployments, and intentions.
2. Fuse data collected from all sources and distribute timely, filtered information to users.
3. Flow friendly information efficiently in the face of enemy attacks and competing friendly requirements.
4. Degrade enemy information networks.[7]
5. Defend friendly information networks against enemy intrusion.

To accomplish these goals, the JFICC should have operational control (OPCON) over certain forces on a routine basis, and should exercise temporary operational control over forces normally under the OPCON of other component commanders.…

Caution: Whenever a new type of warfare emerges, there's a tendency to overstate its case. For example, during the 1920s and 1930s, airpower zealots overstated the capabilities of airpower. Airpower visionaries, such as Douhet and Mitchell, made promises about the future effect of airpower that (to put it charitably) experience was slow to validate. The potential of strategic airpower was easier to foresee than to execute.

Information zealots will likely make similar mistakes. Because societies and militaries are increasingly dependent on information, the potential for information campaigns to fundamentally impact future war is obvious. However, its practice will take time to mature. This delay will be due to uneven progress in military reliance on information technologies, the ability to militarily affect information, and the military's acceptance of the attendant cultural changes.

For example, at the strategic level of war, information will have a decisive effect only if the target state is information-based. If it's a third wave state, its wealth will depend on information.[8] By targeting this information network, a military could impoverish its enemy and facilitate its defeat. However, if the enemy state's wealth is not based on information, a strategic information campaign will not have a decisive effect.…

At the operational and tactical levels of war, however, planners should expect decisive effects from an information campaign. In 1994, the U.S. Army Chief of Staff outlined this point.

> *Information Age armies will develop a shared situational awareness based on common, up-to-date, near-complete friendly and enemy information distributed among all elements of a task force. First, operational and tactical commanders will know where their enemies are and are not.…Of course, this "knowledge" will never be absolute, and it is folly to assume it ever will become "perfect." It will be, however, of an order of magnitude better than that achieved even during the Gulf War. Second, information age armies will know where their own forces are, much more accurately than before—and deny this critical information to the enemy. Last, this enemy and friendly information will be distributed among the forces of all dimensions—land, sea, air, and space—to create a common perception of the*

> *battlefield among the commanders and staffs of information age armies.*[9]

If the United States attains the Army Chief of Staff's vision—while degrading comparable enemy capabilities—it is difficult (though still possible) to envision our defeat. The speed, fidelity, and breadth of modern information systems offer orders of magnitude increases in military efficiency. This efficiency will only increase in the future. As a result, information efficiency will be a key factor in future war and will become an area of conflict. Commanders always seek to observe-orient-decide-act (the "OODA" loop) faster than their opponents. Opposing fighter pilots, JFACCs, and national command authorities (NCA) always try to get inside their opponents' OODA loop. This was true in the past and will remain true in the future. The difference between the past and the future will be in terms of speed and breadth of decisions. As the technical ability to complete the OODA loop in near real time (NRT) emerges, commanders at all levels will move towards ever faster decisions. Whether it will be wise to do so is another question, but the ability to observe and command in NRT will exist—and whoever can get closest to it will gain an advantage.

This drive towards near-real-time C2 will open interesting opportunities for operational art. Commanders will exploit their opponents' drives toward near-real-time decisions. Because near-real-time decisions will require heavy degrees of automation and decision protocols, commanders at all levels will strive to drive their opponent's snap decisions towards poor decisions, usually by presenting false indications of intent or reality.…

This contest over indications offers new possibilities in operational art. By understanding indication priorities and the tendency towards near-real-time ("snap") decisions, a commander could overwhelm the opponent's C2 structure during the critical early phases of the fight.

The ultimate goal in this counter C2 effort will be to compel the opposing force to either slow down its OODA loops or continue making bad decisions in near real time. Either option degrades information efficiency, thus gaining a decisive advantage in war.

Advances in hardware, software, and bandwidth—driven by the private sector—are certain. Their impact on future conflict will be profound. Simply stated, the ability to rapidly exploit observations of friendly and enemy positions and capabilities, at levels superior to that of the enemy, will be decisive at the operational and tactical levels of wars. For this reason, there will doubtless be a fight over information in any future war. Winning this information war—with integrated, redundant, secure, and exercised networks—will be imperative to victory.…

Parallel War

…future aerospace operations against the enemy at all levels of war and across all target categories must occur almost simultaneously. Near-simultaneous attacks across the enemy target set will be the hallmark of future aerospace operations. Failure to conduct aggressive and overwhelming attacks across all facets of enemy power would waste a decisive capability.

The theory of near-simultaneous attack across multiple target sets is nothing new. Airmen have recognized it for decades. A large number of attacks in a day has far more effect than the same number of attacks spread over weeks or months. In his report to President Truman at the end of WWII, General Hap Arnold asserted that strategic air assault is wasted in sporadic attacks that allow the enemy to readjust or recuperate.

Historically, however, airmen lacked the military capabilities to implement near-simultaneous attack. During all of 1942–1943, for example, the Eighth Air Force attacked a total of only 124 distinct targets.[10] At this low attack rate (averaging six days between attacks), the Germans had ample time to repair and adapt between raids.

Contrast this WWII rate of attack with the 1991 Gulf War. In the first 24 hours of Operation Desert Storm, coalition air forces attacked 148 discrete targets. Fifty of these targets were attacked within the first 90 minutes.[11] Targets ranged from national command and control nodes (strategic) to key bridges (operational) to individual naval units (tactical). The goal was to cripple the entire system to the point it could no longer efficiently operate, and to do so at rates high enough that the Iraqis could not repair or adapt. Coalition forces, knowing an incredible amount about Iraq, efficiently orchestrated thousands of sorties, reached key vulnerabilities with high certainty, and, once in the target area, hit specific targets. The end result was near-simultaneous attack across hundreds of key Iraqi targets. Under this intense attack, Iraq was unable to either regain the initiative or orchestrate a cohesive defense.

Such targeting, conducted against the spectrum of targets in a compressed time period, is called parallel war. The goal of parallel war is to simultaneously attack enemy centers of gravity across all levels of war (strategic, operational, and tactical)—at rates faster than the enemy can repair and adapt. This is a new method of war. Previous generations of military strategists could not prosecute parallel war. They had only the sketchiest knowledge of the enemy's key strategic and operational targets. The enemy was opaque prior to contact…

Even when military commanders knew what to target, they had to first "roll back" an enemy's defenses before attacking key centers of gravity. But modern technology is changing these long-held axioms of war. Although it will never be absolutely complete, the Information Age is providing ever increasing details on the strategic and operational centers of gravity of potential enemies. As demonstrated in the Gulf War, modern penetration and precision can place these centers of gravity under massive attack on day one of the war—and do so faster than an enemy can react. Most importantly, modern command and control systems can plan and direct this offensive in near real time.…

Parallel war is enabled by emerging advances in four key technologies:

1. Information. By 2010, well into the Information Age, aerospace planners will detect an incredible amount of information about the target state. They will never know everything, but they will detect orders of magnitude more about the enemy than in past wars. At the

strategic level of war, they should observe the connectivity among the national leadership, the architecture of the national communications grid, and the position of elite troops who are key to regime protection, among other things. At the operational level of war, they should see the location and connectivity of key corps and air defense headquarters, the naval order of battle, the location and LOCs of theater-level supplies, and the coordinates of critical nodes in airfields and ports. At the tactical level of war, they should know where most of the enemy’s unit headquarters are, their communications centers and means, and the individual locations and readiness levels of squadrons, divisions, and ships.

2. Command and Control (C2). Future commanders will use the Information Age’s revolutionary advances in information transfer, storage, recognition, and filtering to orchestrate attacks and defenses. Theater-wide taskings will flow with unprecedented fidelity and speed. Commanders will convert “the understanding of the battlespace into missions and assignments designed to alter, control, and dominate that space.”[12]

3. Penetration. Units will launch penetrating platforms against these targets. Enabled by stealth, hypersonic, and/or electronic warfare technologies, these platforms will penetrate in significant numbers. While defenses will certainly defeat some attackers, others will get

through at rates higher than previously experienced.

4. Precision. Once over the target area, penetrating platforms will deliver brilliant munitions. Deliveries will be highly accurate. Target locations will be measured within feet. Circular error of probability (CEP) will be less than a meter. Brilliant sensors will have the ability to distinguish between tanks and trucks, between parked bombers and decoys. Because of this precision, fixed and mobile targets will be struck by the thousands.

Attacks facilitated by advances in information, C2, penetration, and precision will occur within the first 24 hours of conflict—and continually thereafter. This compressed, broad, and precise attack should leave the opponent paralyzed, unable to either coordinate an effective defense or mount an orchestrated offense. The potential for parallel war will only increase in the future. Information, C2, penetration, and precision will allow targeting of each target type at the outset of hostilities. Advances in the underlying technologies will multiply the number of targets struck.

In 1995, the Air Force Chief of Staff described parallel war as a revolutionary development: “Not too far in the next century, we may be able to engage 1,500 targets within the first hour, if not the first minutes, of a conflict….We will be able to envelop our adversary with the simultaneous application of air and space forces.”[13] Unfortunately for the United States, enemies will also have this capability. Employing—and defending against—parallel attack by aerospace forces will be a crucial aspect of future joint campaigns.

Revolution in Military Affairs

Modern warfare is in the midst of a revolution in military affairs (RMA)….RMAs are more than just changes in technology. Rather, RMAs occur only when militaries fundamentally change their concepts of operations (CONOPS) and their organizational structures to best employ radically new technologies. RMAs are underwritten by technology but realized through doctrinal change.[14] As the U.S. Secretary of Defense noted in 1995:

> *Historically, an RMA occurs when the incorporation of new technologies into military systems combines with innovative operational concepts and organizational adaptations to fundamentally alter the character and conduct of military operations.[15]*

Throughout history, militaries have reacted differently to new technologies. Some opted to overlay new technologies on top of their current ways of doing business. They used new technologies to improve the efficiency of what they were already doing. Other militaries recognized the same new technologies as drivers of fundamental change. To realize the full benefit of the new technologies, they remade themselves; they remade their doctrine and their organization. In so doing, they gained substantial battlefield advantages over those who only overlaid new technologies on top of existing doctrine.…

…Today's aerospace planners face decisions of similar magnitude. Fundamentally new technologies are emerging. They will underwrite the next RMA. However, we won't realize the next RMA unless we devise new ways to employ the mix of emerging and present technologies, plus build organizational structures best suited to support this mix.

What are today's emerging technologies? There are four: information, C^2, penetration, and precision. Future commanders will amass an incredible amount of data about the conflict arena, and they will have the technical means to cycle high-fidelity taskings in near real time. Weapons will reach targets throughout the depth and breadth of the theater and, after penetrating, these weapons will hit exactly where they're aimed. Previous generations of military leaders had bits and pieces of these capabilities, but they never had them all. The synergistic use of these technologies offers the potential for an RMA.

If history is any guide, aerospace forces must devise radically different CONOPS and supporting organizations to realize the full potential of the coming radically new technologies. It will be a singular stroke of luck if current U.S. aerospace CONOPS and organizations bridge the gap between current and future technologies. Devising fundamentally new CONOPS and organizational structures will prove tremendously difficult, however. It will challenge career paths, hard-won modernization programs, professional military education, and a host of other facets crucial to success in war. Nevertheless, confronting this challenge is a prerequisite for realizing this revolution in military affairs.

Complicating our search is the fact that these technologies aren't secret. Both sides in a future war will have access to the same underwriting technologies. Both will have greatly improved information, C2, penetration, and precision. Both may have innovative employment concepts and organizations. Therefore, planners must not only devise ways to use these new technologies; they must also make their operational concepts capable of succeeding while under attack from similar enemy capabilities….

Caution: There is a natural tendency within today's military to focus on *defeating* these new technologies. We speak of information denial, viruses, antistealth radars, and spoofing technologies as having the potential to negate these emerging technologies. By orienting our defenses on these new types of threats, some argue, we can continue to rely on existing concepts of operations—concepts that have proven successful in past wars. Such thinking is a serious mistake….

The successful generals and admirals of our next wars will be the ones who understand that advanced capabilities in information, C2, penetration, and precision are here to stay. We can—and will—increase the vulnerabilities of these technologies, but we'll never make them obsolete. We must resist the temptation to believe that better defenses will allow us to return to the old and proven ways of doing business. Advanced information, C2, penetration, and precision are integral to future war; we must adapt to thrive in their environment….

Peer Competitor

…Fortunately, the chance of war with a peer is remote. The United States has unquestioned military superiority over all possible adversaries. No potential peer nation is arming for war with the United States. The United States currently exceeds every defense budget in the world by at least a factor of four, spending as much on defense as the next eight largest defense budgets in the world combined….[16]

Unfortunately, this favorable environment won't last. If history teaches us anything, it teaches us times change. Despite current optimism, humankind has not seen the end of major war. Major war may happen in 10 years (unlikely), or 15 years (possible), or sometime after that (virtually certain). Defense planners should regard conflict with a peer as inevitable; only the timing is unknown. For discussion purposes, this [excerpt] assumes the early edge of the window—it discusses war with a peer beginning in 2010….

…To envision this future war, planners should start with possible future weapon systems as their baseline—not what is currently on the ramp and in procurement. As the WWII experience shows, most of today's weapons will be obsolete for a 2010 war….

Although today's weapons will become obsolete, today's thinking will not. The doctrines developed today will be critical. If the World War II analogy holds, doctrines developed today will guide rearmament and initial operations in the next war. Today's planners will develop the operational concepts for a 2010 war; how U.S. aerospace forces fight tomorrow will be guided by how U.S. aerospace planners think today. For this reason, we need to explore the concept of war with a peer competitor in the 2010 time frame.

Environment

When projecting a major conflict with a peer, planners must expect both sides to employ significant numbers of advanced-technology aerospace systems. These systems will include:

1. Atmospheric and space-based reconnaissance and communications systems. These systems will vary in quality and quantity between opponents. They will, at a minimum, be able to detect massive force movements and relay this information in near real time despite significant enemy countermeasures.

2. Information Age command and control systems. Future C2 will devise and direct integrated taskings with high fidelity in near real time. They'll be heavily automated and dispersed. Attacks on any single node of this structure will not have catastrophic effects.

3. Stealth aircraft and stealth cruise missiles. Both sides will deploy tens of thousands of aerospace weapons with low signatures. These very low-observable weapons will use state-of-the-art electronic warfare systems to further increase their chances of penetration. Stealthy cruise missiles will be inexpensive, allowing their employment in massive numbers.

4. Precision weapons. Reflecting current trends in sensor technologies, precision weapons will have less than 1 meter accuracy with brilliant munitions.[17] They will guide independently of external positioning systems (e.g., global positioning system [GPS]), and they will have automatic target recognition capabilities.[18] Some of these weapons will retain their accuracy regardless of weather or darkness.

In addition to these emerging technologies, both sides will possess large numbers of nuclear weapons plus delivery systems capable of worldwide reach. This strategic nuclear threat will significantly constrain military operations.…

War with a future peer will present challenges of a different nature from those posed by an MRC scenario today. Both sides will use multiple sensors to detect large force movements and relay this information in near real time to stealthy aerospace weapon systems. Possibly operating from a sanctuary, these stealthy aerospace weapons will likely penetrate aerospace defenses in significant numbers. Once in the target area, they will strike with great accuracy. Most importantly, these weapons will be employed and controlled in an innovative fashion. Both sides will employ emerging technologies in ways that maximize their unique capabilities. Defense forces will face a combination of advanced surveillance and communications, innovative command and control, stealthy attack systems, precision munitions, nuclear weapons, and robust resources in the hands of an innovative attacker.

The fact that this warfighting environment will be challenging and destructive does not mean U.S. aerospace forces can't surmount it. Quite the contrary. If the United States plays its cards right, it could thrive in this environment. The United States already possesses early generations of the key emerging technologies. For example, the United States is experimenting with fourth generation stealth aircraft while other nations are still trying to understand stealth's basic physics. Stealth ownership allows the United States to devise counters and improvements to stealth in practice while others must rely on theory. In addition to stealth, the United States leads most potential enemies in precision weapons, space platforms, all-weather enabling technologies, information war, and simulation. As a result of this head start, the United States can refine and integrate a series of key emerging technologies while other militaries are still trying to build them.…

Today’s aerospace planners must devise superior employment concepts for future weapons. Given the United States lead in technology and resources, the United States should have superior weaponry in a war with a peer. Whether the United States will have a superior CONOPS is less certain. In building a future CONOPS, planners should start by forecasting future weapons capabilities for the United States and its peers.…

As a first step, we should ask ourselves: Will the current U.S. air defensive CONOPS suffice against a peer in 2010? Unfortunately, the answer is probably “no.”

The current air defense CONOPS for all American military forces assumes beyond visual range (BVR) detection of enemy aircraft and missiles. We assume that long-range sensors, primarily radar and infrared, will detect and track enemy aircraft and missiles far from the target area. Given this long warning time, air defense C2 will have time to sculpt a response. We further assume that commanders will have sufficient time to pick the most efficient weapon, task that weapon in a positive manner, and perform cross-checks to decrease the chance of fratricide. For example, current U.S. weapon systems are built on the assumption that long-range sensors will acquire the target. Patriot, AIM-7, AIM-120, and AWACS assume that the target has a high radar signature; DSP and AIM-9 assume that the target has a high infrared signature. Thus, a key assumption throughout the current aerospace control CONOPS is that enemy aerospace platforms will reflect or emit high signatures.

Unfortunately, that assumption will not prevail; future warfare will involve thousands of stealthy cruise missiles and aircraft with low signatures. The heat signatures of aircraft and cruise missiles will be below the tolerances of spaced-based infrared surveillance systems, making them difficult to detect upon launch. Stealth technologies will decrease their chance of detection by radar. In addition, aircraft and cruise missiles will avoid intense defenses by varying their routes. Even if detected in flight, their target will be uncertain. For all of these reasons, alerting specific terminal defenders will be difficult.

Our present CONOPS also assumes limited numbers of attacking missiles and aircraft. Due to the multimillion dollar unit costs of aircraft and accurate ballistic missiles, we can assume that any attack by these systems will be limited. For example, the entire U.S. Air Force (active duty, guard, and reserve) inventory totals only 6,814 aircraft.[19] While large in a relative sense, this number is small in an absolute sense. A limited inventory means limited attacks. Attacks can involve only a few hundred at a time; at most a thousand. Reflecting this limitation, coalition air forces launched only 931 attack sorties during the first 24 hours of *Operation Desert Storm*.[20] Given these relatively limited numbers, the current aerospace defense CONOPS is appropriate. A few hundred costly attackers justifies multiple defensive shots by less expensive (but still costly) SAMs and AIMs. Stealthy cruise missiles, however, change this exchange ratio.

Stealthy cruise missiles are cheap. One U.S. defense contractor reported his company could build a –30db (front and rear aspect) cruise missile with 300 NM range for $100,000. He then added that one should not buy this missile from his company; a company with less overhead could build the same missile much cheaper.[21] Expected advances in production technologies combined with economies of scale (driven by large procurement runs) should cut the costs of very low-observable cruise missiles even further….

Another factor that must be considered is command and control. Current C2 concepts for U.S. aerospace defense are ill-suited to the emerging environment. With few exceptions (e.g., Patriot batteries in automatic mode against incoming missiles), lethal attacks on aerospace targets require human decisions. Human fingers control every trigger. Usually, voice commands are required prior to missile launch. In an era of multiple penetrating targets, each with low signatures, such positive control may prove insufficiently responsive. Only an automated C2 structure will have the speed to react in sufficient time to defeat a mass attack by low-signature missiles. Unfortunately, the culture of current aerospace organizations will slow the understanding of this shortfall.

Another C2 shortfall is in the area of doctrine. U.S. adherence to the doctrine of decentralized execution will degrade defensive operations.[22] Because of the increasing range of defense weapons, multiple defenders may fire on the same target at the same time. They may all have the motivation and opportunity to engage the same target simultaneously. Different batteries of SAMs and flights of interceptors may also overlap coverage of specific targets. We need to deconflict firing decisions across our broad array of defensive weapons in this environment.

Given a fast, lethal, and low-signature target, several defenders may feel the need to quickly take any shot that presents itself. Given decentralized C2, several aircraft/batteries might fire on the same target simultaneously. Or one platform might shoot while another makes a counter-productive maneuver. Or no one might shoot, each thinking that another defender has the lead. The most appropriate defender may even withhold its fire due to fears of threats yet to appear. Low-signature targets pose a considerable problem for future defenders.…

For all of these reasons, sophisticated stealth in the hands of a peer enemy would render our current aerospace defense CONOPS obsolete. If the United States attempts to use its current air defense CONOPS against a future peer aerospace threat, it would not be able to enforce air supremacy.[23] Stealthy attackers would likely penetrate in high numbers.…

In this same context, we must also review future offensive operations. Will the current U.S. offensive CONOPS suffice in the future? Unfortunately, the answer again seems to be “no.”

The current U.S. aerospace CONOPS anticipates extensive use of in-theater systems. The overwhelming majority of these in-theater systems (e.g., AWACS, KC-10, F/A-18E, F-15E, Army Tactical Missile System [ATACMS]) emit or reflect high signatures. If employed against a future peer, they would be highly vulnerable to detection by multiple layers of enemy sensors. With this information, the peer enemy will inflict substantial attrition. Stealthy interceptors (whether manned or unmanned) will attack the airborne platforms. Stealthy cruise missiles and bombers will attack their bases. Short-legged U.S. stealthy systems, such as TLAM, F-22, and F-117, would also be vulnerable. While survivable in flight, they depend on high-signature support systems (e.g., surface ships, AWACS, air refuelers, fixed air bases). By attacking these high-signature support systems, a peer enemy could significantly degrade short-legged U.S. stealth. These vulnerabilities point to a recurrent theme in future warfare theory: high-signature systems won't survive. This theme applies to aerospace forces as well as their ground and naval cousins.

The stealthy cruise missile symbolizes this threat. Future stealthy cruise missiles will:

1. Fly against critical targets;

2. Penetrate into target areas in large numbers; and

3. Hit within feet of their targets.

Stealthy cruise missiles, properly supported by information and precision technologies, will make high-signature, immobile forces extraordinarily vulnerable.…

…In summary, today's aerospace planners must devise a future aerospace CONOPS with three projections in mind. First, aerospace defenses must anticipate a massive, low-signature target set. CONOPS that assume long-range detection of limited attackers will not thrive. Second, offensive aerospace forces must deemphasize high-signature, theater-based forces. Their attrition in the emerging environment will be sufficiently high to preclude high-tempo operations. Third, planners must take steps to induce greater crisis stability into the U.S. force structure and CONOPS. Absent greater redundancy and more effective defenses, the United States could find itself in a “use or lose” predicament during a crisis.

With these three themes in mind, the following 11 operational concepts will be critical to aerospace operations in a future war with a peer:

- Conduct a defensive counterstealth campaign.
- Degrade enemy cruise missile guidance.
- Establish ballistic missile defense.
- Control and exploit space.
- Integrate ISR (intelligence, surveillance, reconnaissance) systems.
- Support the Information Campaign.
- Conduct offensive strikes within enemy homeland.
- Attack enemy invasion/occupation forces.
- Avoid deployment of critical targets within range of enemy stealth.
- Position JFACC in CONUS.
- Airlift critical supplies and spare parts into the combat area.

Support the Information Campaign

Aerospace forces should expect heavy taskings in support of the Joint Force Information Component Commander's (JFICC) campaign. Satellites, UAVs, and manned aircraft will collect data on the enemy's information and C2 architectures. Satellites and UAVs will relay this data to the JFICC's fusion and analysis centers. These centers will identify priorities and critical nodes within these architectures, which the JFICC will use to orchestrate offensive and defensive campaigns. In support of these campaigns, aerospace platforms (ASATs, missiles, bombers) will deliver munitions (both lethal and nonlethal) against JFICC-directed targets. Other military forces will also support the JFICC's campaign, but aerospace forces should expect sizable taskings.

This support will be a part of the theater CINC's normal apportionment process. The CINC will apportion a certain percentage of sorties to JFICC support (e.g., a certain percentage of UAV sorties on a certain day will fly in accordance with JFICC taskings). Just as aerospace forces are sometimes apportioned to support naval or ground campaigns, future information campaigns will see the joint force information component commander tasking aerospace forces in accordance with the theater CINC's overall guidance. The CINC will integrate this information campaign with ground, naval, and aerospace campaigns to effect a strategic victory.

At the same time, the peer enemy will be conducting its own IW campaign against the United States. A prime target will be U.S. military forces. Therefore, U.S. aerospace forces must operate efficiently while under information attack.

The peer will undoubtedly attempt to corrupt information vital to U.S. aerospace operations. The enemy's IW effort will probably center on four general areas:

1. deployment (e.g., the Federal Aviation Administration [FAA] network);
2. employment (e.g., the air tasking order [ATO], battle management);
3. surveillance (e.g., downlinks from ELINT satellites); and
4. logistics (e.g., supply requests).

To mitigate the effects of such intrusion, aerospace forces must incorporate a series of defensive measures. These measures should include regular exercises in a corrupted information environment, software protocols which flag nonstandard inputs, redundant information links which check message fidelity while providing back up information routing, and extensive encryption that is changed regularly. Despite these efforts, we should expect at least modest success by enemy IW….Key to successful operations in any war will be decision cycles. Both sides in a peer conflict will attempt to detect and task in near real time. Each will attempt to make snap decisions—faster and better than its opponent. Whoever builds the tighter decision loop will gain a significant advantage. This struggle for tighter decision loops will occur at all levels of war. Opposing fighter pilots (tactical), JFACCs (operational), and NCAs (strategic)—all will try to observe-orient-decide-act faster than their opponents. Each side will strive towards near-real-time decision cycles because they confer warfighting advantages.

The advantage of near-real-time decisions carries with it a risk. Near-real-time decision cycles will require extensive use of automation and threat/opportunity triggers. By understanding either the algorithms inherent in the enemy’s automated decision architecture or the key factors which trigger certain reactions, the commander can manipulate enemy responses. Therefore, a concerted effort to understand and exploit the enemy’s decision process is mandatory. If effective, such an operation would initially drive the enemy toward bad decisions. After a series of bad decisions, the enemy would be forced to insert added cross-checks into its decision process, thus slowing down its decision cycle. As a result, snap decisions may be poor….

Summary

…The following aspects of future peer warfare deserve special emphasis:

- Aerospace defenses must anticipate massive numbers of low signature attackers. If unit costs of cruise missiles decrease to the $100,000 range, both sides will likely employ large numbers of very low-observable attackers.

- Offensive aerospace forces must de-emphasize high-signature, theater-based assets. Their attrition in the emerging environment will be sufficiently high to preclude high-tempo operations.

- Planners must take steps to induce greater crisis stability into the U.S. force structure and CONOPS, especially with regard to space.

Absent greater redundancy and more effective defenses, the United States could find itself in a first strike predicament during a crisis.

- Planners must avoid deployments of critical fixed targets within range of enemy stealth. Fixed facilities will face an unacceptable risk of destruction by precision stealth systems.

- Planners should integrate satellites and UAVs for communications, navigation, and surveillance. UAVs promise sufficient loiter times—and survivability—to accomplish these missions. Integration will allow rapid substitution and reduce the effects of deception (through cross-checking).

- Space will be a center of gravity in any future war with a peer. Both sides will rely on satellites for communication, positioning, and collection. Satellites in LEO will be particularly vulnerable. They will require both active and passive defenses, including shielding, maneuverability, rapid replacement, frequency management, and redundancy. Satellites in GEO will be secure if enemy launch facilities capable of GEO reach are destroyed.

- Future peer aerospace forces will include stealthy interceptors. As a result, high-signature atmospheric platforms (e.g., AWACS, J-STARS) will not thrive in a future war with a peer.

- JFACC should base in CONUS. Fixed, permanent basing will allow immediate tasking of worldwide assets while excluding a high-value, high-signature target (JFACC HQ) from the range of enemy stealth systems.

- JFACC will provide NRT information on allied and enemy maneuvers to allied forces. This transfer will require specialized equipment and liaison teams.
- Satellites are lucrative targets absent (active and passive) defensive measures.
- Defensive counterair must emphasize sensor fusion. Because a significant portion of the enemy aerospace force will be stealthy—and stealth systems in flight will intermittently reflect and emit—a thoroughly fused sensor network is important. It holds the possibility of successful detection and targeting. This system must be mobile to preclude targeting by ballistic missiles.
- Degrading enemy cruise missile guidance will be a top priority. By manipulating external guidance systems (such as GPS), and by positioning decoys in the target area, defenders will attempt to exploit any algorithm weaknesses in the enemy system.
- Planners must devise a concentrated offensive against key targets within the enemy homeland. C4I is the highest priority. The NCA will probably restrict these strikes due to the threat of nuclear retaliation. For this reason, nonlethal weapons, delivered by stealthy bombers and cruise missiles, will assume a leading role.
- The aerospace campaign will attempt to deny enemy invasion/occupation, primarily through

long-range bombers with precision munitions and cruise missiles. Logistics will be the most lucrative target set.

- When airlifting critical supplies and spare parts into the combat area, operators must minimize ground times. Depending upon distance from enemy missile launchers, ground times will usually be measured in terms of minutes, not hours. Airlift must be capable of efficient operations despite an information-corrupted environment (to include nonavailability of GPS).

- Future aerospace forces will attack critical enemy targets in a parallel fashion, denying their ability to adapt or repair in advance of subsequent strikes. Their goal will not be attrition; they will attempt to paralyze enemy C2.

- Defenses will take advantage of ballistic missile vulnerabilities (large infrared signature at launch, radar reflective in flight, minimal maneuverability). Having said that, a 100 percent shield is probably impossible.

- Aerospace forces should expect heavy taskings in support of the joint force information component commander’s (JFICC) campaign. Operations will center on (1) destroying nodes (such as collection platforms, relay networks, and fusion centers) and (2) distorting information by viral insertion and spoofing. Because the enemy will also conduct IW, aerospace forces must prepare to fight in an information-corrupted environment.…

Niche Competitor

…A niche competitor is a state (or alliance) that combines limited numbers of emerging weapons with a robust inventory of current weapons, then develops an innovative CONOPS to best employ this mix. Examples of possible niche competitors include Iraq and North Korea.

There are five key points to remember when envisioning a niche competitor. First, a niche would always be militarily inferior to the United States. It would have a weaker military and it would have a weaker strategic position. By the former, we mean the niche would never have the breadth and depth of weapons available to the United States. A niche could never hope to slug it out toe-to-toe with the United States. It would inevitably lose an all-out war. Its goal would be to raise the cost of U.S. involvement beyond an acceptable level.…

Second, the niche will present operational centers of gravity to attack. We can assume the niche is doing something outside its borders that is contrary to substantial U.S. interests. That is the casus belli for U.S. military involvement. The invasion/occupation involved in this aggression must be of sufficient size to gain and hold territory. The invading forces would require personnel and equipment numbering in the tens of thousands. These operational forces would present numerous critical targets for attack. Their detection and targeting would be a prime mission for U.S. aerospace forces.

Third, many nations have the capacity to attain niche status. Unlike a peer competitor, a niche seeks to develop a proficiency in only a few mission areas, as opposed to many.…

Fourth, a niche would have to be capable of doing more than fielding state-of-the-art weapon systems. Modern weapons underwrite the ability to compete in the new warfare environment, but are not enough in themselves. To take full advantage of the capabilities inherent in emerging weapons, a niche military must be able to adjust its CONOPS as well as its inventory. For example, a niche must do more than simply buy information weapons. Rather, it must integrate information war systems with the rest of its inventory in a synergistic way. We must expect the niche to employ and control new technologies in innovative ways. These ways might differ markedly from their past doctrine.

Finally, unlike war with a peer, war with a niche will be a “come as you are” war. The absence of risk to U.S. vital interests would preclude domestic American support for a rapid buildup.…Niche competitors will face a similar situation. They’ll have military requirements unrelated to a war with the United States. For domestic and regional reasons, niche competitors will be unable to focus their military efforts solely on defeating the United States. In fact, only a small proportion of their military will be optimized for defeating U.S. forces. Niche states will have more important military missions than just war with the United States.…

In summary, a niche could compete with the United States by employing bits and pieces of advanced technology along with a robust inventory of traditional weapons. It would integrate these weapons using innovative strategies to offset the greater military breadth and depth of the United States. Its goal would be to persuade the United States to leave the conflict (as opposed to seeking a decisive military victory). The niche would exploit asymmetries in strategic culture, geography, and political/military objectives. Warning time for this war would be much shorter than that envisioned for a peer conflict.

Environment

When projecting a future conflict with a niche competitor, the United States must expect the enemy to field a mix of emerging and previous systems, as well as to use an asymmetric method of employment. The types of information, C2, penetration, and precision systems, as well as the number and size of their weapons of mass destruction help to distinguish niche competitors. Table 1 compares the capabilities of a peer competitor to those of a niche competitor.

	PEER COMPETITOR	**NICHE COMPETITOR**
Information	Indigenous, Dedicated	Third Country, Commercial
C2	NRT, Redundant, Automated	Delayed, Nodal, Hierarchical
Penetration	Multisystem	Single System
Precision	Autonomous Guidance (e.g., terminal)	External Guidance (e.g., GPS)
WMD	Hundreds--Can Reach U.S.	Less Than 10--Theater Reach
Size	Large, Strategic Depth	Small, Little Depth

Table 1. Niche Competitor Compared to Peer Competitor

Emerging Systems

In general terms, a niche might have emerging systems with access to commercial satellite (COMSAT) networks (communications and surveillance), modern C2 systems, stealthy cruise missiles (equipped with either warheads or sensors), advanced missile guidance, and advanced conventional munitions. In more specific terms, a niche's emerging systems would emphasize information, C2, penetration, and precision.

A niche enemy will use a mix of civilian and military information systems for military purposes. It will use civilian surveillance satellites to detect large U.S. force movements. Data obtained from civilian sensors will not be near real time (NRT); it may be several days old. Despite its age, such data will prove useful in identifying large, fixed, build-up areas (e.g., airfield parking ramps, logistics points, lines of communication, ports). Civilian communication satellites will relay military data and instructions. Cruise missiles will have surveillance and communications packages to augment satellite coverage.

Owing to expected advances in the civil sector, niche C2 will exceed the current state of the art. Advances will be most significant in the areas of processing, fusion, and encryption. Due to its reliance on civil systems, niche C2 will be delayed relative to our own. It might also present single-point failure nodes and a hierarchical planning and tasking process.

It's a near-certainty future niche competitors will field stealthy cruise missiles. They are currently under development by a wide variety of sources. Any nation with a moderate defense budget should be able to buy several thousand stealthy cruise missiles capable of strike, communications relay, and surveillance.…

A niche enemy will have a large inventory of precision weapons. Reflecting at least mid-1990s state of the art, these weapons will have less than 10-meter accuracy. They may depend on U.S.-controlled navigation systems (e.g., global positioning systems). Some of these weapons will retain their accuracy regardless of weather or darkness.

Previous Systems

A niche's previous systems might consist of a handful of nuclear weapons, large stocks of chemical weapons, a limited number of ballistic missiles, and substantial numbers of late-generation traditional systems (e.g., tanks, aircraft, artillery, surface warships, mines).

A niche competitor would likely have a robust inventory of currently (mid-1990s) available weapons. These could include infantry, armor, artillery, submarines, mines, nonstealthy fighter aircraft, surface-to-air missiles, ASATs, chemical munitions, and short-range ballistic missiles (e.g., Scuds). The niche would use these previous systems to conquer territory, while using its emerging systems to combat U.S. intervention.…A niche competitor would probably have a limited number of nuclear weapons (less than 10). Without an intercontinental ballistic missile (ICBM), however, these weapons would not directly threaten U.S. territory. Nevertheless, they'll threaten U.S. allies and bases in the region.…

…Putting all of these factors together, a niche competitor of 10-20 years from now will present challenges of a different nature from those posed by an MRC-scale competitor today. A future niche will be able to detect large U.S. force deployments and relay this information to stealthy weapon systems. These systems will likely penetrate U.S. aerospace defenses in significant numbers. Once in the target area, they'll strike with great accuracy. This combination of previous weapons (tanks, a few nuclear weapons, submarines, ASATs, surface-to-air missiles, etc.) plus emerging weapons (stealthy cruise missiles, civil satellites for reconnaissance and communications, etc.), orchestrated by a new CONOPS, would confront U.S. aerospace forces with a demanding situation.

Asymmetric Employment Schemes

Further complicating this environment would be the likelihood of asymmetric employment schemes. A niche competitor would likely avoid a direct confrontation with the United States. Rather, the niche would attempt to offset U.S. strengths by employing an indirect strategy. For example, a niche competitor would not seek information dominance. It is highly unlikely a niche will surpass the U.S. military in information technologies over the next 10-20 years….Therefore, the niche might pursue an "information neutral" environment. It would attempt to "level the playing field" by degrading U.S. information flows.

Information leveling could be accomplished several ways. One way would be through hackers. The niche could hire any number of computer hackers to attack U.S. information networks. These hackers could be hired at the last minute, assuring state-of-the-art competence. They could be hired in large numbers from around the world; India and Russia, for example, have a wealth of software talent willing to work for relatively low pay. It would be very difficult for the United States to assess the scope and direction of this campaign in advance of hostile intrusion.

Fortunately, such an offensive has significant weaknesses. For example, the United States could take steps to protect its vital information systems. Just as banks and businesses protect their information systems through encryption and protocols, the U.S. military would use similar methods to protect its information systems. Another weakness is that disorganized hackers would probably bring little orchestration to their attacks. Lacking proper training and positive control, they would likely "service" targets with little regard to operational art. Finally, hackers would get little feedback on success or failure. They would not know whether they were successful; nor could they be sure they were entering a real system. Despite these weaknesses, however, hackers in the employ of a niche could pose a credible threat to U.S. information systems. Serious defenses are mandatory.

A second approach to information leveling would be by physical attacks on U.S. collection and communications satellites. The niche could launch primitive ASATs against these platforms, particularly those in low earth orbit. The niche could also detonate a nuclear weapon in space or in the upper atmosphere. The resulting electromagnetic pulse (EMP) would disable unshielded satellites. Replacement satellites, if also unshielded, would quickly degrade due to the enhanced radiation retained by the Van Allen Belts.[24] While niche systems in space would also be affected, EMP blasts would probably adversely affect U.S. information forces—and thus, U.S. operations—to a greater extent than those of the niche aggressor. An orchestrated campaign with ASATs and EMP blasts could degrade U.S. space systems and cripple U.S. military operations worldwide.

A third asymmetric employment strategy available to a niche is projection denial. Niche competitors will not have the means to conduct a long-range campaign against U.S. forces with a high confidence of success. They would lack the NRT intelligence and manned penetrators necessary for such a campaign. However, niches could offset these shortcomings by combining a mix of relatively low-tech systems and weapons to make U.S. power projection operations difficult, or even unfeasible. For example, a niche could mix a handful of modern diesel submarines and mine barriers to slow and canalize U.S. sea lift. It could observe the resulting choke points with commercial overhead imagery then target specific ships with stealthy cruise missiles.…

Should the United States decide to absorb these attacks and remain in the war, it would face a decision. The United States could either operate under this type of observation or attempt to interdict the niche's information. The latter would prove difficult in the Information Age where multiple sensors outside government control are available. Data—and its means of transmission—is becoming ubiquitous. It seems most likely the United States will be forced to operate under a limited amount of enemy observation. Prudent aerospace planners should allow for this probability.

By employing innovative operational concepts and a limited number of emerging weapons, a niche competitor could pose significant challenges to U.S. operations in certain circumstances. Asymmetric employment concepts, particularly in the areas of information and power projection denial, might “level the playing field” to the point the United States is dissuaded from involvement. To deal with this challenge, U.S. aerospace forces should prepare to employ the following 10 operational concepts:

- Paralyze enemy command and control.
- Dominate battlefield awareness.
- Integrate space-based systems and unmanned aerial vehicles for conflict surveillance.
- Support the information campaign.
- Attack enemy wealth.
- Attack enemy invasion/occupation forces.
- Establish aerospace superiority.
- Avoid deployment of critical fixed targets within range of enemy stealth.
- Airlift forces and logistics into the combat area.
- Support the ground counteroffensive.

Paralyze Enemy C2

…For a niche competitor, command and control nodes are a major vulnerability. Modern U.S. surveillance systems (especially electromagnetic intelligence) are expert at identifying command links. Open-source literature can also provide wiring diagrams of communication flows. Once identified, these nodes are vulnerable to U.S. attack.

There is little a niche competitor can do to forestall this vulnerability. If the niche constructs a command and control network comprised solely of hardened, indigenous systems, it will be, at best, rudimentary. The United States could easily operate within the niche enemy's decision loop. If, at the other extreme, the niche uses world-class communications systems and protocols, it will expose itself to massive information interdiction. This interdiction could be remarkably precise.…

The United States will strike enemy C2 nodes at each level of war. At the strategic level of war, national political and military leadership will be attacked. The goal will be to isolate the enemy's national decision makers from their instruments of power. These instruments may range from weapons of mass destruction, to air defense, to intelligence, to political control over their population. The niche's nuclear weapons should not sway this strategy. As long as the U.S. effect is to isolate the enemy leadership from its means of command—as opposed to decapitation—the United States can avoid placing enemy leadership in a suicidal corner.

At the operational level of war, field commanders will be severed from their subordinate units. At the tactical level, units will be cut off from their battle managers. Threat warnings and targeting information will arrive too late to do any good.

Dominate Battlefield Awareness

…This concept has three components. First, platforms continuously surveil the area of interest. A mixture of aircraft, satellites, and UAVs, equipped with multispectral sensors, establishes 24-hour, all-weather coverage of the battle area. Unattended ground sensors sniff/watch/listen/ report along areas of possible maneuver. SOSUS-type sensors listen for underwater threats. Second, data generated by these sensors are fused and filtered through wide-area automatic target recognition software. This software cues more refined systems to specifically identify emitters and high-signature targets (e.g., armored formations or logistics points). Lastly, this information is disseminated to weapon systems. This dissemination takes advantage of large bandwidth and digital compression technologies. It transmits via direct broadcast satellites. The result of these three steps is dominant battlefield awareness.

Integrate Space-based Systems and UAVs for Conflict Surveillance

Niche competitors will probably have the ability to target satellites in LEO and to effect an EMP burst in space (via a nuclear explosion). The United States must have ready counters for these probabilities. Of the two, the EMP threat may be the lesser challenge. Satellites must already be hardened due to solar activity. This shielding could be intensified to negate EMP effects. However, this shielding would be required on all satellites for which military operations are dependent—including civilian-owned communications satellites.…

…the United States must augment space-based systems with atmospheric systems. Fortunately, UAVs, along the lines of Tier II+ and Tier III-, are well along in development. High altitude-long endurance UAVs, with loiter times of 48-72 hours, are probable in our planning time frame. They promise sufficient loiter times and survivability to accomplish the surveillance mission. While UAVs have capabilities that recommend them in their own right, they are also necessary to provide redundancy for space-based systems. Satellites in LEO with predictable trajectories are simply too vulnerable to interdiction.…

Support the Information Campaign

Dominant battlefield awareness also requires denying the enemy a similar amount of information. As with a peer enemy, the theater CINC will task the Joint Force Information Component Commander to orchestrate a denial/distortion campaign. In a sense, the JFICC will deprive the information age to the niche. Once that's accomplished, the other components will end the industrial age.

Against a niche competitor, we should expect the JFICC to conduct a short, high-tempo information campaign. This is due to two factors. First, the niche's information target set would be smaller than that of a peer. By definition, a niche would be less robust in information infrastructure. Second, because the niche would not pose a likely nuclear threat to the United States, fewer political restrictions on homeland attacks will come into play. This would permit attacks with all types of conventional munitions across all target categories. The result should be a short, intensive campaign on a limited number of targets in the most efficient way possible.

Aerospace forces would directly support this campaign. In most cases, targets should be highly precise. They would include connectivity (e.g., fiber-optic lines and radio/cellular antennas), nodes (e.g., switching stations), repair assets, downlink stations (e.g., satellite ground stations), fusion centers, and C2 personnel. Munitions used against these targets will cover the gamut of the inventory—earth penetrators, MHD, EMP, CBU, HE, etc. Bombers and cruise missiles would serve as delivery platforms.…

Attack Enemy Wealth

To undercut the niche's ability to continue the war and to punish it for starting the war in the first place, the CINC would probably direct aerospace forces to attack the niche's wealth. If the niche depends on trade, aerospace forces would identify and interdict that trade.…

Attack Enemy Invasion/Occupation Forces

…U.S. Defense Department planning guidance in 1993 described notional niche invaders as having at least 5,000 armored vehicles and several hundred thousand troops.[25] Such massed formations of tanks, troop carriers, and mobile artillery—necessary for all but a dispersed, foot borne invasion—are readily detected. Once detected, they are vulnerable to aerospace attack. Bombers and cruise missiles, carrying a wide assortment of precision munitions, have a proven ability to destroy massed, slow-moving surface forces. Practically the entire family of aerospace munitions under current development (sensor fused weapons, wide-area munitions, brilliant antitank munitions) is optimized for this target set. Equipped with advanced munitions either in service or about to become operational and directed by modern C3I systems, airpower has the potential to destroy enemy ground forces either on the move or in defensive positions at a high rate while concurrently destroying vital elements of the enemy’s warfighting infrastructure….[26]

…Precision munitions delivered with an element of surprise against enemy logistics should have a devastating effect. A major goal of U.S. aerospace forces will be to “hollow out” an attacking army by gutting its logistics…U.S. aerospace forces would concentrate on countering military invasions by striking an invader’s maneuver forces, logistics, and C4I from the outset of hostilities.…

Establish Aerospace Superiority

We should expect niche competitors to field a limited number of ballistic missiles; many already do (e.g., Scuds). The speed, range, and survivability of mobile ballistic missiles make them attractive. Planners must incorporate the ballistic missile threat within their calculus when devising future aerospace superiority regimes. Fortunately, ballistic missiles in the hands of a niche competitor should have several major weaknesses.

One weakness is that ballistic missiles offer a high signature.…

Another weakness is that ballistic missiles are expensive.…A third weakness is that mobile targets are almost invulnerable to ballistic missiles.…Lastly, while ballistic missiles are optimized for attacking targets with limited windows of vulnerability, this capability demands an extensive support network. This support network must include surveillance sensors, sensor-to-warhead target data transmission, and an NRT decision cycle. Such a network adds to unit costs and presents a lucrative target set for U.S. attack.…

Manned aircraft in the hands of a niche competitor is probably the easiest aerospace defense task. During the time period of this projection, the United States will face only nonstealthy fighters….This lack of stealth availability means niche air forces must rely on nonstealthy fighters. These fighters can't compete with the F-22. Thus, any niche confronting the United States will find itself with a significant quality disadvantage in terms of air-to-air fighters.…

Having said that, numerous stealthy cruise missiles will almost certainly penetrate even the most robust defenses. Therefore, it's doubtful the United States will be able to establish air supremacy if the niche has a substantial inventory of stealthy cruise missiles employed from mobile launchers.…

Airlift Critical Supplies and Spare Parts into the Combat Area

A major difference between a peer competitor and a niche competitor is the niche's absence of near-real-time sensor-to-shooter systems. When fighting a niche, we can assume there will be a delay in the cycle time necessary for the niche to detect a U.S. vulnerability, make an attack decision, disseminate the tasking, and put a weapon on target (time of flight). As long as airlift ground times are shorter than this time loop, airlift operations can proceed.…

Support the Ground Counteroffensive

…Just as Hitler left von Paulus' Sixth Army at Stalingrad and Saddam left his conscript divisions to be run over in the Kuwaiti theater of operations, we must anticipate that niche enemies would leave their invasion forces in place regardless of the effectiveness of air strikes against them. If these forces occupy territory of interest to the United States or its allies, friendly ground forces would eventually have to launch a counteroffensive to drive them out.…

The following aspects of niche warfare deserve special emphasis:

- We must avoid deployments of critical fixed targets within range of enemy stealth. Their risk of destruction by stealth systems would be unacceptable.

- JFACC should base in CONUS. This fixed, permanent basing will allow immediate tasking of worldwide assets while excluding a high-value, high-signature target (JFACC HQ) from range of enemy stealth systems.

- LEO satellites would be lucrative targets absent extensive defensive measures. Satellites in GEO will be easier to defend; we can minimize a niche’s limited GEO ASAT capability by attacking its space launch infrastructure.

- To undercut the niche’s ability to continue the war and to punish it for starting the war in the first place, the CINC would probably direct aerospace forces to attack the niche’s wealth. Targets could include trade, resources, and/or services. Assets of the ruling elites would have top priority.

- During the time period of this projection, the United States would face only nonstealthy fighters. It’s unlikely a niche would have stealthy aircraft. In addition, any niche would face a serious shortfall in numbers. Even assuming a 1:1 exchange ratio, any niche would lose its frontline fleet and pilots without any hope of quick replacement.

- The United States must augment communications and reconnaissance satellites with unmanned atmospheric systems. UAVs promise sufficient loiter times and survivability to accomplish these missions. JFACC would forward NRT information on friendly and enemy maneuvers to allied forces. This transfer would require providing technical support and liaison officers.

- Degrading enemy cruise missile guidance would be a top priority. By manipulating external guidance systems such as GPS and by positioning decoys in the target area, defenders would attempt to exploit any algorithm weaknesses in the enemy system.

- Defenses would take advantage of ballistic missile vulnerabilities (large infrared signature at launch, radar reflective in flight, minimal maneuverability). Having said that, a 100 percent shield is probably impossible.

- We must mount a concentrated offensive against enemy C4I. Cruise missiles and stealth bombers would assume this mission.

- Our defensive counterair campaign would emphasize sensor fusion. Enemy stealth systems would intermittently reflect and emit in flight, especially from the side and rear aspects. A thoroughly fused sensor network holds the possibility of successful detection and tracking.

- Aerospace forces would support the JFICC campaign. All niche vulnerabilities would be targeted from the onset of the war. Aerospace taskings would likely be heavy.
- The aerospace campaign would attempt to deny enemy invasion/occupation, primarily through long-range bombers and cruise missiles delivering precision munitions.
- When airlifting critical supplies and spare parts into the combat area, we must minimize ground times. Depending upon distance from enemy missile launchers, ground times should be measured in terms of minutes, not hours.
- Aerospace forces would support counteroffensive forces. A counteroffensive would probably be necessary to reclaim territory from the aggressor.
- JFACC would attack the niche in parallel. All target types at all levels of war would come under attack near simultaneously. The goal of these attacks would not be attrition. Rather, the goal would be paralysis, especially of the enemy's C2.

…many of these aspects of a future CONOPS differ significantly from that currently envisioned for MRC planning.…The implications of this environment deserve extensive examination and debate.

Near-Term Actions

This work is only a first attempt at building a vision of future aerospace warfare. A more accurate and comprehensive vision is needed. An institutional effort will be required for the U.S. Department of Defense to build and implement this vision. Three initiatives would considerably promote this institutional effort:

1. Designate a focal point for future warfare. A vision of future war is important to today's decision makers; the fact one doesn't exist reveals a serious shortcoming….

2. Build a concepts development center (CDC). This center would have the sole, permanent mission of developing operational concepts for future warfare….

3. Build an information warfare center. This should be a new organization dedicated to developing warfighting concepts for the Information Age. It should deal with all forms of information war (strategic/operational/tactical; offensive/ defensive; all missions)….

Immediate Action

In addition to these broad efforts to clarify our vision of future war, five narrower actions are appropriate for immediate implementation.

1. Task Defense Intelligence Agency for comprehensive future projections. The Defense Intelligence Agency (DIA) does a good job of estimating worldwide arms inventories and force structure trends. That effort should continue. However, future capabilities of possible adversaries involve more than weapons inventories. How a military intends to operate is also important. Therefore, DIA should also focus

on trends in doctrine (as revealed by writings, HUMINT, exercises)….

2. Study out-of-theater C2. Our present CONOPS deploys C2 to the theater of operations. The CINC and component commanders deploy close to the fight. This concept made sense when proximity to the battle was necessary to obtain accurate information. However, high-value C2 nodes within range of enemy stealth systems is an ever-increasing risk. Also, C2 deployments delay development and implementation of campaign plans during transit and setup. Since today's joint C4I architecture makes accurate information available at great distances, it is now possible to command forces from greater distances….

3. Study centralized control of national and theater collection platforms. National and theater surveillance systems are poorly integrated. They are tasked separately. Much of their output feeds separate databases. Because future enemies will target our information systems, these systems must function together. Should one go down, another must immediately take up the slack. This can best be done by a centralized command authority….

4. Organize for information war. IW has offensive and defensive aspects. It is conducted at the strategic, operational, and tactical levels. It has many subsets (e.g., jamming, viruses, psyops). Unfortunately, no one is responsible for bringing the art of war to IW in its entirety. NSA has a piece. So do SPACECOM, the services, each

CINC, and so forth. Because information supremacy will be as important as air supremacy to future war, it's time to designate a CINC for IW. This CINC will work IW at the strategic and operational levels of war (components will retain tactical-level IW—just as they retain tactical aircraft while the AF works strategic and operational airpower). CJCS should designate CINCSPACE as the IW "king…."

5. Organize for parallel war. General Fogleman spoke of the possibility of attacking 1,500 targets the first day of a war. If his vision is correct, we're looking at far more than just an increase in efficiency—we're looking at the possibility of a new style of warfare. Future war may be conducted by attacking an enemy across all target sets and all levels of war near simultaneously. This type of war could strip an opponent of the ability to repair and adapt.…

Required Flexibilities

Future warfare will also require specific flexibilities within weapon systems. Decisions made today will affect that flexibility. Therefore, today's acquisition considerations for aerospace forces should include these factors:

- Information. Platforms must have the ability to incorporate/upgrade the latest information hardware and software, employ information obtained by off-board sensors, and transmit information garnered by onboard sensors to other weapon systems. Systems must also be able to operate despite a corrupted information environment.

- Long range. Aerospace platforms should be based as far from enemy stealth systems as possible. Distance either puts a base out of enemy stealth range or gives layered defenses more opportunities to detect and target enemy attacks. Short-range systems will contribute only in very low-threat environments.

- Stealth. High-signature aerospace weapons won't survive in future war. Weapon systems must emphasize passive sensing, minimal reflectivity, and discrete emissions. If platforms have these characteristics but their support structures (e.g., tankers, AWACS, fixed air bases) do not, the platform as a weapon system will not survive.

- Precision. Manned aerospace platforms will become increasingly expensive. Driven by their need to incorporate long range, stealth, data processing, and mobility, there's no way they will also be cheap. This expense will drive down inventories. At the same time, target sets are expanding (better C2 will allow dispersion; the possibility of strategic attack adds to the number of targets). There's also the desirability of conducting near-simultaneous attack across all levels of war. Precision is required to reconcile these trends. Each sortie must kill multiple targets.

- UAVs. We need to think in terms of tens of thousands of UAVs. Their inherent stealthiness and minimal basing requirements allow low-signature operations. Their lack of an aircrew allows casualty-indifferent operations.…They are increasingly capable of long-endurance flights. They can perform strike, communications, and surveillance missions. While manned platforms will remain mandatory for certain types of missions, UAVs will make decisive contributions to future aerospace operations if employed skillfully in large numbers.…

- Mobility. One result of the Information Age will be the enemy's near-certain detection of fixed facilities. To offset this information, future commanders will need the flexibility to move land-based aerospace forces between bases. Such mobility requires a lean support structure. This concept affects how we envision munitions, C2, maintenance, POL, and support equipment.

- Alternatives to space. Satellites in fixed orbits will be exceedingly vulnerable in the future. Military operations dependent on satellite support rest on a dubious assumption of satellite survivability. We need alternatives to space-borne architectures. These alternatives should emphasize HALE UAVs and fiber-optic cable.

- Power projection. Finally, the Information Age will fundamentally affect power projection. Ubiquitous sensors and transmission devices will give our future military commanders extensive information on the enemy's scheme of maneuver. Unfortunately, the enemy will also have substantial information about our forces. This information will make either side's invasion forces exceptionally vulnerable when they mass

> to attack. Mobile defenses accompanying massed forces will be inadequate to stop interdiction forces emphasizing state-of-the-art information, C2, penetration, and precision. It is at this point, very early in the battle, that wars will be won or lost. Once territory is seized, it may prove excessively costly to reclaim. Therefore, future U.S. weapons must be capable of "day one" operations. U.S. weapons must have the capacity to strike with overwhelming force from the first day of the war.

[1] Adm William A. Owens, "Vision Force 2005: The Pending Revolution," Briefing, Vice Chairman Joint Chiefs of Staff, March 1995.

[2] Inserting false data into an enemy's information system is probably the most effective tactic in information war. It encourages the enemy to: (1) mistrust all its data; and (2) construct internal barriers (or gateways) for data entry.

[3] *Foreign Broadcast Information Service (FBIS)-CHI-93-126*, July 2, 1993, p. 22.

[4] Vladimir I. Slipchenko, "A Russian Analysis of Warfare Leading to the Sixth Generation," *Field Artillery* (October 1993), p. 38.

[5] In a similar vein, all components employ aircraft, but only one (the Air Force) has the primary missions of strategic attack and defeat of the enemy's air force.

[6] Secretary of the Army Michael P. W. Stone, *Preliminary Report, Lessons from Operations Desert Shield and Storm*, April 22, 1991, p. 7. Entire report is classified (Secret). Information extracted is unclassified.

[7] Richard O. Hundley and Eugene C. Gritton, *Future Technology-Driven Revolutions in Military Affairs* (Santa Monica, Calif.: RAND, 1994), p. 68.

[8] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little Brown, and Co., 1993). First Wave states are agrarian-based. Second Wave states are industrial-based. Third Wave states are information-based.

[9] Gordon R. Sullivan and James M. Dubik, "War in the Information Age," *Military Review* (April 1994), p. 56.

[10] Roger A. Freeman, *Mighty Eighth War Diary* (London: Jane's Publishing Co., 1981), pp. 9-161.

[11] CENTAF Master Attack Plan, 16 January 1991. Although the plan is classified, these figures are unclassified.

[12] Adm William A. Owens, “The Emerging System of Systems,” *Proceedings* (May 1995), p. 38.

[13] Gen Ronald R. Fogleman, “Getting the Air Force into the 21st Century,” speech to the Air Force Association’s Air Warfare Symposium, Ireland, Florida, February 24, 1995. Italics and underlining in the original.

[14] For a more complete overview see James R. FitzSimonds and Jan M. van Tol, “Revolutions in Military Affairs,” *Joint Force Quarterly* (Spring 1994), pp. 24-31.

[15] William J. Perry, *Annual Report to the President and the Congress* (Washington, D.C.: Department of Defense, 1995), p. 107.

[16] *The Military Balance, 1994-1995* (London: The International Institute of Strategic Studies, Brassey’s, 1994). The United States budgeted $261.7B for defense for FY 1994. The next eight largest defense budgets (in order): Russia ($79B); Japan ($42B); France ($35B); United Kingdom ($34B); Germany ($28B); Italy ($16B); South Korea ($14B); and Saudi Arabia ($14). Total: $262B. China’s military budget is difficult to state with precision. *The Military Balance* estimates somewhere between $7B to $27B (see p.170). Note: Dollars for defense are not an absolute gauge of military capability. They are only a rough indicator. However, ratios of 4, 8, or 20 to 1 suffice to preclude military equivalence.

[17] Brilliant sensors can discriminate between targets (e.g., identify a tank versus a truck).

[18] Full ATR under all weather conditions is foreseen within 10 years. See *AviationWeek & Space Technology*, February 6, 1995, p. 20.

[19] “USAF Almanac 1995,” Air Force Magazine, May 1995, 50. Figure is TAI (Total Aircraft Inventory).

[20] Office of the Secretary of the Air Force, *Gulf War Air Power Survey*, Volume 5, 1993. (Secret) Information extracted is unclassified.

[21] Proprietary conversation between OSD/NA and a corporate vice president of a major U.S. defense contractor, May 1995.

[22] *Air Force Manual (AFM) 1-1, Basic Aerospace Doctrine of the United States Air Force*, Volume 1, fig. 2-2. “Centralized Control/ Decentralized Execution” is a “Tenet of Aerospace Power.” “Execution of aerospace missions should be decentralized to achieve effective spans of control, responsiveness, and tactical flexibility.”

[23]*AFM 1-1*, Volume 2, defines air supremacy as “That degree of air superiority wherein the opposing air force is incapable of effective interference.” Air superiority is “That degree of dominance in the airbattle of one force over another which permits the conduct of operations by the former and its related land, sea, and air forces at a given time and place without prohibitive interference by the opposing force.”

[24]R.C. Webb, et al., “The Commercial And Military Survivability Crisis,” *Defense Electronics*,” (August 1995), pp. 21-25.…

[25]Les Aspin, *Report of the Bottom Up Review* (Washington, D.C.: U.S. Department of Defense, October 1993), p. 13.

[26]Christopher Bowie, *The New Calculus* (Santa Monica, CA: RAND, 1993), pp. 83-84.

CHAPTER 14

NETWORK-CENTRIC WARFARE:

ITS ORIGIN AND FUTURE

By
Arthur K. Cebrowski and John J. Garstka

Arising from fundamental changes in American society and business, military operations increasingly will capitalize on the advances and advantages of information technology. Here at the end of a millennium we are driven to a era in warfare. Society has changed. The underlying economics and technologies have changed. American business has changed. We should be surprised and shocked if America's military did not.

For nearly 200 years, the tools and tactics of how we fight have evolved with military technologies. Now, fundamental changes are affecting the very character of war. Who can make war is changing as a result of weapons proliferation and the fact that the tools of war increasingly are marketplace commodities. By extension, these affect the where, the when, and the how of war.

We are in the midst of a revolution in military affairs (RMA) unlike any seen since the Napoleonic Age, when France transformed warfare with the concept of levee en masse.[1] Chief of Naval Operations Admiral

Jay Johnson has called it “a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare,”[2] and it will prove to be the most important RMA in the past 200 years.

Network-centric warfare and all of its associated revolutions in military affairs grow out of and draw their power from the fundamental changes in American society. These changes have been dominated by the co-evolution of economics, information technology, and business processes and organizations, and they are linked by three themes:

- The shift in focus from the platform to the network
- The shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem
- The importance of making strategic choices to adapt or even survive in such changing ecosystems[3]

These themes have changed the nature of American business today, and they also have changed and will continue to change the way we conduct the sometimes violent business of the military. We are some distance from a detailed understanding of the new operations—there is as yet no equivalent to Carl von Clausewitz’s *On War* for this second revolution—but we can gain some insight through the general observation that nations make war the same way they make wealth.

The Underlying Economics Have Changed

The organizing principle of network-centric warfare has its antecedent in the dynamics of growth and competition that have emerged in the modern economy. The new dynamics of competition are based on increasing returns on investment, competition within and between ecosystems, and competition based on time. Information technology (IT) is central to each of these. The U.S. economy has been on a steady growth path generally attributed to the emergence of larger global markets, the globalization of labor and capital, and the widespread application of information technology within business enterprises.[4] To get an idea of the magnitude of investment in information technology, consider the fact that the information technology sector—only a small fraction of the economy (3 percent in 1996)—has been the largest contributor to growth in gross domestic product. In 1996, its contribution was 33 percent, with an average of 27 percent over the past three years.[5] Within this sector, competition based on increasing returns has emerged as a new dynamic.

The preponderance of competition in the economy is characterized by decreasing returns on investment. Referred to here as “Economy A,” it is characterized by stability, market share equilibrium, and decreasing returns on investment. Competing products or services are interchangeable, and multiple companies provide roughly comparable goods and services. As a result, there is no mechanism for product lock-in. Efforts to increase market share yield decreasing returns on investment because of constraints in intellectual capital, physical plant, or distribution or because of the response of a competitor.

Competition based on increasing returns is different. “Economy B” is the much smaller but much discussed part of the economy characterized by extraordinary growth and wealth generation, increasing returns on investment, the absence of market share equilibrium, and the emergence of mechanisms for product lock-in.[6] It is the engine for America's powerhouse economy. Competing products are based on competing standards, are not necessarily interoperable, or require skill sets that are not easily transferable. This is especially true of key types of information technology, such as video cassette recorders, personal computers, and communications technology. In addition, in key sectors of Economy B, the laws of supply and demand that govern Economy A have been turned on their heads. As demand for personal computers increases, for example, price for constant performance decreases.

In Economy B, a product or product standard attains such a dominant position that consumers drop competing products because of concerns about the availability of "content" or product support or because they prefer a familiar product based on existing skills or content. In the case of the typewriter, lock-in was based on the skill set associated with the "QWERTY" keyboard. For the VCR, lock-in was based on the VHS price/performance advantage over Beta and was reinforced by the content providers' decision to release movies in VHS format. Everyone who bought Beta switched and lock-in was achieved.

With personal computers, lock-in of the Windows-Intel (WINTEL) standard emerged as a result of multiple factors that combined to reduce the initially dominant Apple Computer technology to a niche. An important early advantage was a new business computing application (the spreadsheet) optimized to run on the DOS-Intel standard introduced by IBM. In the first three months after the introduction of Lotus 1-2-3, IBM's PC sales tripled. This initial success was reinforced by a superior licensing strategy, the emergence of PC clones, and the decision by software vendors to develop applications first for the ecosystem with the largest market share—WINTEL.[7]

Locking-out competition and locking-in success can occur quickly, even overnight. We seek an analogous effect in warfare.

The Underlying Technologies Have Changed

Information technology is undergoing a fundamental shift from platform-centric computing to network-centric computing. Platform-centric computing emerged with the widespread proliferation of personal computers in business and in the home. The significant investment the IT sector makes in research and development and product development (in some cases up to 18 percent of sales) has led to key technologies that have created the conditions for the emergence of network-centric computing.

This shift is most obvious in the explosive growth of the internet, intranets, and extranets.[8] Internet users no doubt will recognize transmission control protocol/ internet protocol (TCP/IP), hypertext transfer protocol (HTTP), hypertext markup language (HTML), Web browsers (such as Netscape Navigator, and Microsoft's Internet Explorer), search engines, and JavaTM Computing.[9] These technologies, combined with high-volume, high-speed data access (enabled by the low-cost laser) and technologies for high-speed data networking (hubs and routers) have led to the emergence of network-centric computing. Information "content" now can be created, distributed, and easily exploited across the extremely heterogeneous global computing environment.

Network-centric computing is governed by Metcalfe's Law, which asserts that the "power" of a network is proportional to the square of the number of nodes in the network.[10] The "power" or "payoff" of network-centric computing comes from information-intensive interactions between very large numbers of heterogeneous computational nodes in the network. Sun Microsystems may have been the first to point out that it is not so much about the computer as it is about the computer in the networked condition. Under fierce competitive pressure, and sensing a strategic opportunity in this fundamental shift in computing, IBM Chairman Lou Gerstner announced that IBM was moving to network-centric computing.[11] The compelling business logic for this shift in strategy was the opportunity for IBM to link its heterogeneous computing lines more effectively and provide increased value for its customers. This is the same value proposition we seek in warfare.

The Business of America Has Changed

The emergence of the dynamic and unstable Economy B has changed the American way of business significantly. First, many firms have shifted their focus to the much larger, adaptive, learning ecosystems in which they operate. Not all actors in an ecosystem are enemies (competitors); some can have symbiotic relationships with each other. For such closely coupled relationships, the sharing of information can lead to superior results.

Second, time has increased in importance. Agile firms use superior awareness to gain a competitive advantage and compress timelines linking suppliers and customers. Even firms that operate in Economy A have found ways to harness Economy B technologies and techniques to increase efficiency and productivity. Central to these developments is the shift to network-centric operations, which are characterized by information-intensive interactions between computational nodes on the network. Whether these interactions are focused on commerce, education, or military operations, there is “value” that is derived from the content, quality, and timeliness of information moving between nodes on the network.[12] This value increases as information moves toward 100 percent relevant content, 100 percent accuracy, and zero time delay—toward information superiority.

Dominant competitors across a broad range of areas have made the shift to network-centric operations—and have translated information superiority into significant competitive advantage[13]—but the benefits are particularly apparent in transaction-intensive operations, such as retailing and securities trading. Wal-Mart and Deutsche Morgan Grenfell are two firms that have made the shift to network-centric operations. Both have gained tremendous competitive advantages by co-evolving their organizations and processes to exploit information technology. Characteristic of big winners, they employ network-centric operational architectures that consist of a high-powered information backplane (or information grid), a sensor grid, and a transaction grid. These architectures provide the ability to generate and sustain very high levels of competitive space awareness, which is translated into competitive advantage.

Leading U.S. firms have come to understand and employ this network calculus well.

The shift from platform to network is what enables the more flexible and more dynamic (and profitable) network-centric operation. Therefore, the construction of high-quality networks is their top priority. The shift from viewing partners as independent to viewing partners as part of a continuously adapting ecosystem increases speed and profitability in both sales and production. Therefore, they have developed high-speed sensor grids and automated command-and-control systems closely coupled with their transaction grids. The key to market dominance lies in making strategic choices appropriate to changing ecosystems. Simply pursuing operational effectiveness while adhering to an obsolete strategy is a formula for failure.

How Can the Military Not Change?

Network-centric operations deliver to the U.S. military the same powerful dynamics as they produced in American business. At the strategic level, the critical element for both is a detailed understanding of the appropriate competitive space—all elements of battlespace and battle time. Operationally, the close linkage among actors in business ecosystems is mirrored in the military by the linkages and interactions among units and the operating environment. Tactically, speed is critical. At the structural level, network-centric warfare requires an operational architecture with three critical elements: sensor grids and transaction (or engagement) grids hosted by a high-quality information backplane. They are supported by value-adding command-and-control processes, many of which must be automated to get required speed.

Network-centric warfare enables a shift from attrition-style warfare to a much faster and more effective warfighting style characterized by the new concepts of speed of command and self-synchronization. Attrition is the traditional “Economy A” analogue because it yields decreasing returns on investment. Reversals are possible, and frequently the outcome is in doubt.

Network-centric warfare, where battle time plays a critical role, is analogous to the new economic model, with potentially increasing returns on investment. Very high and accelerating rates of change have a profound impact on the outcome, “locking-out” alternative enemy strategies and “locking-in” success. There are two complementary ways that this is accomplished:

- Network-centric warfare allows our forces to develop speed of command.

- Network-centric warfare enables forces to organize from the bottom up—or to self-synchronize—to meet the commander’s intent.

Speed of command has three parts:

1. The force achieves information superiority, having a dramatically better awareness or understanding of the battlespace rather than simply more raw data. Technologically, this will require excellent sensors, fast and powerful networks, display technology, and sophisticated modeling and simulation capabilities.

2. Forces acting with speed, precision, and reach achieve the massing of effects versus the massing of forces.

3. The results that follow are the rapid foreclosure of enemy courses of action and the shock of closely coupled events. This disrupts the enemy's strategy and, it is hoped, stops something before it starts.

One of the strengths of network-centric warfare is its potential, within limits, to offset a disadvantage in numbers, technology, or position.

Speed of command facilitates the lock-out phenomenon observed in Economy B, but with even more powerful effects. Lock-out often takes years to achieve in business, but in warfare it can be achieved in weeks or less.

The joint suppression of air defense mission provides an example at the tactical level of how the increased combat power associated with network-centric operations can contribute to speed of command and lock-out. The High-speed Anti-Radiation Missile (HARM) is used to suppress or destroy enemy surface-to-air missile (SAM) sites. When we employ platform-centric operations in this scenario, we achieve virtually no kills. The HARM still will suppress the SAM sites—because site operators realize that these missiles are out there and so adjust their behavior—but those sites will stay there through the duration of the war. Consequently, aircraft that carry HARM missiles have to fly throughout the entire campaign, and all strike aircraft continue to be at risk. By shifting to modern digital technology, we can increase battlespace awareness to yield increased combat power, with more targets destroyed. But if, through co-evolution of systems, organization, and doctrine, we introduce other shooters that are capable of attacking SAM sites, such as ATACMS, and employ them as part of an engagement grid, virtually all of the sites can be destroyed in the same amount of time. It is easy to focus on the number of sites destroyed, but the payoff is in the initial very high rate of change. When 50 percent of something important to the enemy is destroyed at the outset, so is his strategy. That stops wars—which is what network-centric warfare is all about.

Military operations are enormously complex, and complexity theory tells us that such enterprises organize best from the bottom-up. Traditionally, however, military commanders work to obtain top-down command-directed synchronization to achieve the required level of mass and fires at the point of contact with the enemy. Because each element of the force has a unique operating rhythm, and because errors in force movement needlessly consume combat power, combat at the operational level is reduced to a step function, which takes time and provides opportunity to the enemy. After the initial engagement, there is an operational pause, and the cycle repeats.

In contrast, bottom-up organization yields self-synchronization, where the step function becomes a smooth curve, and combat moves to a high-speed continuum. The “Observe-Orient-Decide-Act (OODA) Loop” appears to disappear, and the enemy is denied the operational pause. Regaining this time and combat power amplifies the effects of speed of command, accelerating the rate of change and leading to lock-out. Self-synchronization was illustrated during the Taiwan Straits crisis. In 1995, when the People’s

Republic of China attempted to influence Taiwanese elections with some high-quality saber rattling, the United States quickly dispatched carrier battle groups, and the situation seemed to settle out. For our purposes, the most exciting part of that story was the fundamentally different way that command and control was exercised. Then-Vice Admiral Clemins, as Commander, Seventh Fleet, and his subordinates reduced their planning timelines from days to hours. This order of magnitude change suggests that something very fundamental is happening.

One reason we say that no plan survives initial contact with the enemy is because situational awareness does not. In platform-centric military operations, situational awareness steadily deteriorates. It is reestablished periodically, but it only then deteriorates again. Network-centric operations such as those used in the Taiwan Straits example create a higher awareness, and allow it to be maintained. Such awareness will improve our ability to deter conflict, or to prevail if conflict becomes unavoidable. This is not just a matter of introducing new technology; this is a matter of the co-evolution of that technology with operational concepts, doctrine, and organization. The enabler, of course, is technology. In the Taiwan case, Admiral Clemins was able to use e-mail, a very graphic-rich environment, and video teleconferencing to achieve the effect he wanted.

We are beginning to see the broad impact of network-centric warfare throughout the fleet, as key technology building blocks are deployed. In early 1997, a single aircraft carrier in the western Pacific sent 54,000 e-mails in one month—about half the amount of all of the traditional message traffic that was sent in Western

Pacific during the same time. That is an example of a very complex outfit organizing itself from the bottom up. Now it is the norm. Such capabilities enable a move into the realm of speed of command. Questions decrease because ambiguity decreases, collegiality increases, and timelines shorten.

The Emerging Logical Model

The structural or logical model for network-centric warfare has emerged. The entry fee is a high-performance information grid that provides a backplane for computing and communications. The information grid enables the operational architectures of sensor grids and engagement grids. Sensor grids rapidly generate high levels of battlespace awareness and synchronize awareness with military operations. Engagement grids exploit this awareness and translate it into increased combat power.[14] Many key elements of these grids are in place or available. For example, at the planning level, the elements of a DoD-wide intranet are emerging. To assure interoperability, all elements of the grids must be compliant with the Joint Technical Architecture and the Defense Information Infrastructure common operating environment. However, their full integration into a more powerful warfighting ecosystem is only partially complete.

This is not theory—it is happening now. For example, new classes of threats have required increased defensive combat power for joint forces. The combat power that has emerged—the cooperative engagement capability (CEC)—was enabled by a shift to network-centric operations.[15] CEC combines a high-performance sensor grid with a high-performance engagement grid. The sensor grid rapidly generates engagement quality awareness, and the engagement grid translates this awareness into increased combat power. This power is manifested by high probability engagements against threats capable of defeating a platform-centric defense. The CEC sensor grid fuses data from multiple sensors to develop a composite track with engagement quality, creating a level of battlespace awareness that surpasses whatever can be created with stand-alone sensors. The whole clearly is greater than the sum of the parts.

How to Get There

No one operates better than the U.S. Navy. Our forward presence force is the finest such force in the world. But operational effectiveness in the wrong competitive space may not lead to mission success. More fundamentally, has the underlying rule set changed so that we are now in a different competitive space? How will we revalue the attributes in our organization?

To choose a sporting example, although the objective of the game, the number of plays, and the operating environment are essentially the same, football is fundamentally different from soccer because its underlying rule set is different. Accordingly, the competitive attributes of mass, continuity of play, self-synchronization, sustained speed, and others are revalued. There are important differences between the ways a soccer coach and a football coach would recruit, train, and organize their teams.[16]

Similarly, if we decide to fight on a network-centric rather than platform-centric basis, we must change how we train, how we organize, and how we allocate our resources. A good understanding of our competitive space, therefore, is vital to achieving success. The Navy, indeed all services, must make these strategic decisions to maximize future combat power and relevance. Because a network-centric force operates under a different, more modern rule set than a platform-centric force, we must make fundamental choices in at least three areas: intellectual capital, financial capital, and process.

Intellectual Capital

Information-based processes are the dominant value-adding processes in both the commercial world and the military. Yet the military fails to reward competence in these areas. "Operator" status frequently is denied to personnel with these critical talents, but the value of traditional operators with limited acumen in these processes is falling, and ultimately they will be marginalized, especially at mid-grade and senior levels. The warfighter who does not understand the true source of his combat power in such things as CEC, Global Command and Control System, and Link-16 simply is worth less than those who do. The services must both mainstream and merge those with technical skills and those with operational experience in these areas. These are the new operators.

Every new revolution in military affairs produces a new elite. The inherent cultural changes are the most difficult and protracted. We must start now. While we delay, our people, our most vital asset, are deciding that they want to compete on a different team.

Financial Capital

Navy decision making across a broad front is aligning with the network-centric warfare strategy. We are moving forward rapidly with ship- and aircraft-launched weapons that have reach, precision, and responsiveness, and advanced C2 concepts are under development.

The Navy's umbrella strategy for enabling the IT elements of network-centric warfare is Information Technology for the 21st century (IT-21). It provides for accelerated implemetation of customer-led command, control, communications, computers, and intelligence (C4I) innovations and existing C2 systems/ capabilities (programs of record). The Navy's commitment to funding IT began in fiscal year 1997. For the fiscal year 1999 budget request and the Future Years Defense Program, Navy funding for IT-21-related programs exceeds $2.5 billion. Battle groups and amphibious ready groups are deploying with increasing network capabilities.

All elements of the network-centric warfare model must move forward if the promise of the revolution is to be realized. Delays will mean higher costs, reduced combat power, and, in the joint arena, failure to achieve the concepts of *Joint Vision 2010*.

Transformation Process

In spite of a ponderous acquisition process, technology insertion is ahead of and disconnected from joint and service doctrine and organizational development. The problem is cultural and systemic. A process for the coevolution of technology, organization, and doctrine is required.

Service experimentation programs are a vital first step. While the temptation may be to take some units out of readiness reporting status for use in an experimental force, the result would be to isolate the larger force from the process. The objective is to create an ethos for experimentation, innovation, and a willingness to risk across the entire force. Specific top-down experimentation will be required because of cost and size or to establish overarching priorities, but these are expected to spawn experiments from the bottom up and facilitate cultural and organizational changes. That is the concept behind the Navy's Fleet Battle Experiment Program.

The concepts of network-centric operations, shifting competitive spaces, changing underlying rule sets, and co-evolution are not mere theory. They have been applied successfully under demanding conditions with encouraging results. Similarly, these concepts are not limited to a few optimum circumstances. The crime rate in New York City, for example, was reduced dramatically through the application of these concepts.

We may be special people in the armed forces, but we are not a special case. It would be false pride that would keep us from learning from others. The future is bright and compelling, but we must still choose the path to it. Change is inevitable. We can choose to lead it, or be victims of it. As B. H. Liddell Hart said, "The only thing harder than getting a new idea into the military mind is getting an old one out."

> *Note: Network-Centric Warfare derives its power from the strong networking of a well-informed but geographically dispersed force. The enabling elements are a high-performance*

information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value-adding command-and-control (C2) processes—to include high-speed automated assignment of resources to need—and integrated sensor grids closely coupled in time to shooters and C2 processes. Network-centric warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is transparent to mission, force size and composition, and geography.

Speed of Command is the process by which a superior information position is turned into a competitive advantage. It is characterized by the decisive altering of initial conditions, the development of high rates of change, and locking in success while locking out alternative enemy strategies. It recognizes all elements of the operating situation as parts of a complex adaptive ecosystem and achieves profound effect through the impact of closely coupled events.

Self-Synchronization is the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up. The organizing principles are unity of effort, clearly articulated commander's intent, and carefully crafted rules of engagement. Self-synchronization is enabled by a high level of knowledge of one's own forces, enemy forces, and all appropriate elements of the operating environment. It overcomes the loss of combat power inherent in top-down command directed *synchronization characteristic of more conventional doctrine and converts combat from a step function to a high-speed continuum.*

[1] The levee en masse was a shift from the previous model of maintaining a small professional army. France was able to take advantage of the changes in society from industrialization to take nearly the entire adult male population to war, transforming the nature of armed conflict during the Napoleonic era.

[2] Address at the U.S. Naval Institute Annapolis Seminar and 123d Annual Meeting, Annapolis, MD, 23 April 1997.

[3] James F. Moore, "The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems," *HarperBusiness*, 1996.

[4] Stephen B. Sheperd, "The New Economy: What It Really Means," *Business Week* 17 November 1997, pp. 38-40.

[5] Michael J. Mandel, et al., "The New Business Cycle," *Business Week*, 31 March 1997, pp. 58-68.

[6] W. Brian Arthur, "Increasing Returns and the New World of Business," *Harvard Business Review*, July-August 1996, pp. 100-109; and *Self-Reinforcing Mechanisms in Economics: the Economy as an Evolving Complex System* (Addison-Wesley, 1988), pp. 9-31.

[7] Robert X. Cringely, "Accidental Empires," *HarperBusiness*, 1992, pp. 139-158.

[8] Amy Cortese, "Here Comes the Intranet," *Business Week*, 12 February 1996, pp. 76-84.

[9] Bud Tribble, et al., "JavaTM Computing in the Enterprise: What It Means for the General Manager and CIO," Sun Microsystems, Inc., white paper.

[10] George Gilder, "Metcalfe's Law and Legacy," *Forbes ASAP*, 13 September 1993.

[11] Ira Sager, "The View from IBM," *Business Week*, 30 November 1995.

[12] "Technology and the Electronic Company," *IEEE Spectrum*, February 1997.

[13] Philip L. Zweig, et al., "'Beyond Bean Counting," *Business Week*, 18 October 1996.

[14] See "The Emerging Joint Strategy for Information Superiority," Joint Staff J-6, information briefing at www.dtic.mil/JCS/J6.

[15] "The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest* 16, 4 (1995): 377-96.

[16] The example was developed by Col. Fred P. Stein, USA (Ret.).

CHAPTER 15

THE SEVEN DEADLY SINS OF NETWORK-CENTRIC WARFARE

By
Thomas P. M. Barnett

Most of us read Vice Admiral Art Cebrowski's seminal 1998 *Proceedings* article on network-centric warfare (NCW), and if some detected a confidence too bold, that is only to be expected. Visions of the future invariably rankle, especially when they seem inevitable. Quoting Liddell Hart, "The only thing harder than getting a new idea into the military is getting an old one out." Admiral Cebrowski and coauthor John Garstka threw down the gauntlet and dared anyone to prove them wrong.

Would that I could, but the best I can muster is a devil's advocate take on what I see as network-centric warfare's seven deadly sins. Note that I don't say "mortal sins." As with any transgression, penance can be made.

Lust: NCW Longs for an Enemy Worthy of Its Technological Prowess

If absence makes the heart grow fonder, network-centric warfare is in for a lot of heartbreak, because I doubt we will ever encounter an enemy to match its grand assumptions regarding a revolution in military affairs. The United States currently spends more on its information technology than all but a couple of great powers spend on their entire militaries. In a world where rogue nations typically spend around $5 billion a year on defense, NCW is a path down which only the U.S. military can tread.

Meanwhile, our relatively rich allies fret about keeping up, wondering aloud about a day when they won't be able even to communicate with us. These states barely can afford the shrinking force structures they now possess, and if network-centric warfare demands the tremendous pre-conflict investments in data processing that I suspect it does, then the future of coalition warfare looks bleak indeed. Not only will our allies have little to contribute to this come-as-you-are party, they won't even be able to track the course of the "conversation."

As for potential peer competitors, forget about it—and I am not just talking money. I am a great believer in the "QWERTY effect," by which technological pathways are locked in by market victories of one standard over another.[1] No one would argue against the notion that the United States is QWERTY Central, or that our military feeds off that creativity. So the reality facing any potential enemy is that he either has to get in line behind our QWERTY dominance or satisfy himself with chintzy knockoffs from our far-distant past. So when Iran gets itself some North Korean missile technology, let's remember that it is only a poor copy of old Chinese technology, which is a poor copy of old Soviet technology, which is a poor derivative of old Nazi-era German technology—and, as everyone knows, our German scientists were better than their German scientists! This is why proliferation is always a lot slower than suggested by too many hyperbolic experts.

Once you get past the potential peer competitors, you are entering the universe of smaller, rogue enemies that many security experts claim will be able to adapt all this information technology into a plethora of brilliant asymmetric responses—the Radio Shack scenario. Frankly, it stretches my imagination to the limit to conjure up seriously destabilizing threats from resource-poor, small states, unless we let our lust for a bygone era distort our preparations for a far different future.

Sloth: NCW Slows the U.S. Military's Adaptation to a MOOTW World

Military operations other than war (MOOTWS) are the closest thing to a sure-bet future the U.S. military faces right now, and network-centric warfare does not yet answer that mail. Beyond the affordability issues, there is the larger question of what "networked" should mean for the U.S. military: Wiring up among ourselves? Or wiring ourselves up more to the world outside?

This is not an esoteric question for naval forces, because I see a future in which the establishment of, and support to, information networks is the crucial U.S. naval product delivered overseas to internal crises where confusion, complexity, and chaos are the norm. We are far more likely to be called on to be the deliverers of clarity and context than sowers of blindness and vertigo, and we are far more likely to be asked to settle down all sides in a conflict than to decimate one particular side. This is where NCW's "lock-out" phraseology misleads: we will be interested in opening up pathways to resolution, not closing down pathways of conflict. That reality speaks to nonlethal approaches, reversible effects, and keeping open the channels of communication.

Increasingly, naval forces will be called on to serve as a “node connector,” rather than a “node destroyer.” I am talking not only about bringing crisis-involved regions back on line, but also about the military acting as Network Central for the wide array of U.S. and international agencies that populate any U.S.-led response to complex humanitarian emergencies. Just as important as our ability to talk among ourselves during the generation and coordination of large-scale violence will be our ability to generate and coordinate the conversations of many outsiders in the prevention of small-scale violence.

Correctly focused, network-centric warfare would allow the U.S. military to come into any crisis situation and establish an information umbrella to boost the transparency of everyone’s actions. Incorrectly focused, it might hamstring us along the lines of the Vietnam War. In sum, NCW’s quest for information dominance is self-limiting in an era that will see the U.S. military far less involved in network wars than in mucking around where the network is not.

Avarice: NCW Favors the Many and Cheap; the U.S. Military Prefers the Few and Costly

Many experts rightly claim that network-centric warfare is nothing new as far as the U.S. Navy is concerned. By its nature, our worldwide, blue-water Navy always has been a networking environment. Of all the major services, it should find the onset of NCW least discombobulating. But it is no secret to anyone who has followed Navy force structure decision making this decade that we consistently have sacrificed ship numbers to technology, even as we decry the resulting stress on operational tempo and global presence.

What we are ending up with is a Navy poorly situated for an NCW era in which the network's crucial strength is its flexibility to degrade gracefully. Some point out that cruise missiles and unmanned aerial vehicles are good fixes because they allow surface combatants to operate in a standoff mode. But the future fleet cannot consist of a dozen huge platforms sitting in the middle of the ocean remotely directing operations because we as a country cannot risk losing any of these hyper-tech behemoths. NCW's bottom line must be that no node can be worth more than the connectivity it provides.

Because we are far more likely to encounter targets of influence operating in the "few and cheap" paradigm, what we should bring to the table are "the many" as opposed to "the costly." Why? The few-and-costly approach puts us in no-win situations, where our entry into crises is self-limited by our tendency—and our opponent's knowledge of that tendency—to treat the loss of any significant network node as grounds for one of two equally bad pathways: escalation or withdrawal. Because our interests typically are limited, escalation usually is the last thing we want. But because the world values our Leviathan-like role as global force of first response and last resort, a pattern of withdrawals over relatively small losses costs us dearly over the long run. A superpower navy too valuable to risk force structure losses is not one worth having. Does that mean we risk more lives? Only if we insist that the U.S. Navy primarily is about projecting destructive power ashore.

Pride: NCW's Lock-out Strategies Resurrect Old Myths about Strategic Bombing

Ever since Giulio Douhet's *Command of the Air* (1921), we have heard that massed effects against an enemy's centers of gravity can lead swiftly to bloodless victory. And every war since then has seen this theory's vigorous application and subsequent refutation. Yet the notion persists and now finds new life in network-centric's "lock-out" strategy. Whether NCW's proponents admit it or not, what lies at the core of this strategy is the spurious notion that punishment equals control.

Can we, by destroying our enemy's information technology "village," somehow save it? I think not.

First, one man's information warfare is another man's international terrorism. If any hostile power tried even a smidgen of what we propose to do en masse via NCW, we would be hurling all sorts of war crimes accusations. The collateral damage associated with this "information technology decapitation" strategy simply is too complex to control from afar. Who dies? Society's weakest and most vulnerable. Unless we are talking total war or some antiseptic battlefield out in the middle of nowhere, we need to own up to the reality that such massed effects are closer to weapons of mass destruction than we care to admit.

Second, our bomb-damage assessment capabilities are nowhere near capable enough to measure the massed effects of NCW's souped-up brand of information warfare. Some assume that the smaller a society's information technology quotient, the greater our ability to understand the impact of information warfare. But in my mind, less information technology equals greater social capacity for low-tech work-arounds that either negate or complicate information warfare immeasurably.

Third, while bowing to complexity theory, NCW adherents toss it out the window once they rhapsodize about lock-out strategies. Somehow, our mastery of our enemy's complexity will translate into a capacity to steer his actions down one path or another, despite the fact that NCW's game plan includes large amounts of irreversible impact. What we may well end up with in some blossoming conflict is a "dialogue of the deaf" that precludes effective communication with the other side concerning conflict resolution or—more important—avoidance of unnecessary escalation. And when that happens, we may wonder which side really had its pathways locked out.

Fourth, NCW is guilty of mirror imaging: we theorize about our own information technology vulnerability and then assume it is the same for others. In reality, our distributed society is far stronger than we realize. In truth, is there any other country in the world where you would prefer to live through a natural disaster? As for less-advanced countries, our arrogant assumptions about their limited work-around capacity say more about us than about them.

Fifth, to the extent that network-centric's immense capabilities can be harnessed to a lock-out strategy, the military needs to relate better to the universe of relevant data and subject-matter experts outside the usual realm of political-military thinking. We do not possess the decision assessment tools at this point to steer an opponent via information dominance.

Anger: NCW's Speed-of-Command Philosophy Can Push Us into Shooting First and Asking Questions Later

The unspoken assumption concerning speed of command seems to be that because we receive and process data faster, we have to act on it faster. Not surprisingly, this virtuous circle can turn vicious rather quickly if commanders allow themselves to become slaves to their own computers, which essentially are dumb machines that count incredibly fast. Rushing to bad judgment is the danger.

Most worrisome are network-centric's assumptions concerning getting inside the enemy's decision loop. This makes sense as a goal, but the real focus should be on what we do once inside, not just on the blind pursuit of faster response times. Why? We always are talking about potential enemies with less advanced information technology architectures, so the potential for miscommunication and misperception is huge. We may find ourselves acting so rapidly within our enemy's decision loop that we largely are prompting and responding to our own signals, which our beleaguered target cannot process. In short, we could end up like Pavlov's dog ringing his own bell and wondering why he's salivating so much.

It takes two to tango, so, yes, we want sufficient speed of command to get inside our opponent's decision loop, but too much speed turns what we hope is a stimulusresponse interaction into a self-stimulating frenzy. The potential irony is telling:

- We rapidly fire signals to a target of influence, who does not pick them up, in part because of the strategic blindness we have inflicted on him.
- Our target's lack of response is interpreted as signifying "X" intent.
- We respond to perceived intent "X" with signal "Y," which also is missed by our target, who, perhaps, is just getting a grip on earlier signals.
- Our target's response "Z" seems incomprehensible, or we assume it is a rejection of sorts to our previous signals.
- Before you know it, we are way beyond "Z" and into some uncharted territory, but we are making incredible time!

The networked organization's great advantage is that the processing and distribution of data are sped up considerably. What this should translate into is increased time for analysis and contemplation of appropriate response, not a knee-jerk ratcheting down of response time. The goal is not to shorten our decision-making loop, but to lengthen it, and, by doing so, improve it. Otherwise, all we are doing is generating two sub-optimal decisions to his one.

Now, some will declare that the enemy's decision loop is being shortened by his increasingly rapid incorporation of information technology into his command-and-control architecture. But this Chicken Little approach misleads: yes, he will improve his decision-loop timelines constantly, and so should we.

But the point is not to engage in some never-ending speed race with our own worst-case fears, but rather to concentrate NCW on how best to exploit the delta between our loop time and his. Speed is not the essence here, only the means to an end. Forget that and you might as well be acting in anger.

Envy: NCW Covets the Business World's Self-Synchronization

There is no defense establishment more concerned with everyone singing off the same sheet of music than the U.S. military. Why? No military in the world seeks to decentralize crucial decision-making power as much. It is both our calling card and our greatest weapon—our operational flexibility. So if any military will adapt itself to NCW's ambitious goal of self-synchronization, it will be us, though we are not likely to reach the ideal state of affairs desired by network-centric warfare, which I believe seeks a dangerous slimming down of the observe-orient-decide-act (OODA) loop.

The implied goal of self-synchronization is that information technology will facilitate such a rapid movement of information as to obviate the time requirements of the "00" portion, allowing commanders to exploit speed of command. But in my mind, NCW's capacity to collapse timelines for the processing of operational data should lengthen the observe and orient portions of the loop, not encourage their virtual disappearance by outsourcing that cognitive function to silicon units. During the Cold War, a sort of "DADA loop" was forced on the U.S. military by certain bolt-from-the-blue warfighting scenarios involving the

Soviet Union. But I am hard-pressed to envision post-Cold War scenarios where the U.S. military should be encouraged to deemphasize the rational thinking that must periodically interrupt whatever courses of action our commanders in the field are empowered to pursue.

NCW's envy for the business world's market-responsive notion of self-synchronization is understandable, for there are few things in this world as complex as a major military operation. But this envy is misplaced; we create governments to deal precisely with those thorny aspects of social life that we do not trust private firms to manage under the ultimate self-synchronizing motivation known as profit seeking. And among the thorniest aspects are those we reserve for the military, entrusted as it is with the assets that generate big violence.

In addition, the crisis scenarios the U.S. military faces grow ever more ambiguous as far as U.S. national interests are concerned. Other than a rerun of Desert Storm, I don't see any crises where the United States would be well served by its military focusing on self-synchronization. A MOOTW world should encourage greater externally focused networking. So even if the U.S. military could achieve self-synchronization, neither the likely scenarios nor the partners we engage in them are well suited to this slam-bang approach. In fact, in many MOOTW scenarios, it is the military that should use its mighty information technology power to generate the "00" portion of the decision loop for others who ultimately will take the lead in deciding and acting.

Gluttony: NCW's Common Operating Picture Could Lead to Information Overload

The term "common operating picture" is apt for network-centric's vision of all players at all levels working off the same mental model. There is little doubt that computer-mediated visual presentations will shape much of the commander's perception of operational realities. That, in and of itself, is not new.

What is new is the potential for inundating all participants with an ever-increasing flow of data masquerading as information because it has been slickly packaged within the common operating picture. The danger lies in the picture's collapsing all participants' perceptions of what is tactical versus operational versus strategic, and, by doing so, creating strong incentives for all to engage in information overload in an attempt to maintain their bearings in this overly ambitious big picture. In sum, I am concerned that the push for speed of command and self-synchronization will drive all participants to an over-reliance on the common operating picture as a shared reality that is neither shared nor real.

The common operating picture cannot really be shared in the sense that ownership will remain a top-down affair. What is scary about NCW's ambition is the strain it may put on commanders at various levels to integrate the commander's intent from all other commanders and not just up the chain of command. NCW promises to flatten hierarchies, but the grave nature of military operations may push too many commanders into becoming control freaks, fed by an almost unlimited data flow. In the end, the quest for sharing may prove more disintegrating than integrating.

The infusion of information technology into hierarchical organizations typically reduces the traditional asymmetries of information that define superior-subordinate relationships. Taken in this light, the common operating picture is an attempt by military leaders to retain the high ground of command prerogative—a sort of nonstop internal spin control by commanders on what is necessarily a constantly breaking story among all participants, given their access to information that previously remained under the near-exclusive purview of superior officers.

That gets me to the question of the common operating picture's "realness," for it suggests that the picture will be less a raw representation of operational reality than a command-manipulated virtual reality. At worst, I envisage command staff engaging in a heavy-handed enforcement of commander's intent, all in the name of shaping and protecting the common operating picture.

The temptation of information gluttony always will be with NCW. Salvation lies in the concept of information sufficiency by level of command.

I seek not to praise network-centric warfare, nor to bury it. To the extent that NCW marries the military to a networking paradigm, it moves America's defense establishment toward a future I view as inevitable. However, focusing NCW on the application of large-scale violence, or past wars, is a mistake-especially for naval forces. On a global scale, both organized violence and defense spending have migrated below the level of nation-states. For our military to remain relevant, it must reach out to that sub-national environment. Networking is the answer, but it needs to be focused outwardly. This was the natural role of naval forces in

U.S. history. It can be again, but only if the Navy frees itself from its Pacific War past and pointless competition with the Air Force in power projection.

[1] QWERTY refers to the first six letters on the upper left of the typewriter keyboard. This layout was adopted late in the 19th century to minimize jamming of mechanical striking arms. It quickly became the universal standard and remains so to this day, despite being less efficient than other designs.

CHAPTER 16

WHAT REVOLUTION IN MILITARY AFFAIRS?

By
William Hoehn

It has become fashionable in national security circles to posit an impending "Revolution in Military Affairs" (RMA) driven by postulated large U.S. comparative advantages in a broad array of information technologies. The thrust of this chapter is that this revolution:

1. is not "impending," nor even near-term;
2. like most information-based technologies, is potentially subject to numerous unexplored and therefore poorly-understood vulnerabilities;
3. commits the United States to the development, procurement, and above all, integration of a "system of systems" in which the success of each mission on the battlefield depends on the accomplishment at every discrete level of a lengthy chain of events;[1]
4. has not been costed, and therefore, even if its technical feasibility were conclusively demonstrated, cannot be shown to be cost-effective relative to alternative force structures;

5. will likely accelerate the movement by potential enemies toward forms of “asymmetric warfare” against which the RMA and traditional U.S. military forces are least likely to be useful; and

6. in the current constrained budget environment, threatens to limit funding for counters to “asymmetric warfare” and to prematurely downplay the importance of well-trained U.S. human operators of high-performance weapons systems.

Introduction to the RMA

The RMA is predicated on the seamless melding of technologies in three major areas: Intelligence, Surveillance, and Reconnaissance (ISR); Command, Control, Communications, Computers, and Information Dissemination (C4I), and Precision Force (PF).

ISR in the RMA postulates the seamless fusing of information from all intelligence and surveillance assets so as to provide 24-hour-a-day, all weather coverage of a theater area (nominally 200 x 200 n. mi.) in such detail as to continuously track, with a position accuracy of less than 10 centimeters, every enemy installation, vehicle, and detachment throughout that battlefield. With such total battlefield surveillance, it is argued, the theater commander will no longer be enveloped in the “fog of war” and can select his strategy and tactics with perfect knowledge about the enemy.

C4I in the RMA postulates a similar seamless integration of all forms of computers and communications devices to provide “infinite bandwidth” to every military user on demand. Whether text or graphics, whether the latest satellite photography or enemy communications intercept, all information will be made available instantaneously to all users. Not only will all information be available to each user, but "intelligent agents" will have sorted, sifted, and prioritized available information for each user, so that each receives his most mission-critical information first.

Precision Force in the RMA postulates the immediate availability of the most effective weapon type to be applied against each enemy target type that a commander wishes to attack, while minimizing the exposure of "own troops" within the theater. Because the enemy's positions are all accurately identified through ISR well before they can achieve close engagement with our forces, they can be attacked and destroyed at a distance. Thus, it is unnecessary to mass large friendly forces for defense of territory, and equally unnecessary to be able to deploy large U.S. forces to deal with contingencies that occur in distant locations. Under the RMA, both weapons delivery platforms and their crews have diminishing relevance, since the necessary survivability, reliability, range and accuracy will all have been built into each weapon type.

Perhaps the most forceful advocate for this "Revolution in Military Affairs" has been Admiral William A. Owens (Retired). As Vice-Chairman of the Joint Chiefs of Staff, Owens oversaw the original development of this concept within the Defense Department and advocated it to the Congress. Since his retirement, he has continued to support the concept. While the most detailed briefings on this topic are classified (a national security topic only gains credibility in Washington if it is classified) and limited largely to

Pentagon and Congressional audiences, many articles on aspects of the RMA have been published. One of the earliest unclassified versions of the RMA argument, co-authored by Admiral Owens, appeared in an article in *Foreign Affairs*.[2]

As an example of the hyperbole that has accompanied the RMA, in testimony before the Senate Armed Services Committee in 1995 while serving as the Vice-Chairman of the Joint Chiefs, Admiral Owens stated that the RMA would be achievable "before the turn of the century."[3] Hyperbole aside, the RMA has now become a "top-down" integrated set of programs in the Pentagon, commanding substantial, and increasing, resources within DoD's annual budgets.

In the eyes of its advocates, the case for the RMA is simple and straightforward. The United States already has a major lead over the rest of the world in the exploitation of many relevant information technologies; computers and networks are ubiquitous throughout industry and government, including the military; and U.S. technical intelligence and surveillance capabilities are robust. Moreover, the U.S. lead in advanced technologies such as "stealth" and "smart" weapons was amply demonstrated to the world during Operation Desert Storm in 1991, and subsequently in attacks using long-range cruise missiles against targets in Iraq, Sudan, Afghanistan, and, more recently, Yugoslavia. To the RMA advocates, all that appears to be missing in order to achieve the capabilities envisioned for the RMA is the "seamless integration" of these various systems and technologies into a "system of systems," along with some modest capability improvements in selected areas.

As evidence of the feasibility of such synthesis, they point to emerging capabilities such as the Navy's Cooperative Engagement Capability (CEC). The CEC is a distributed system of hardware and software which allows each ship within a widely-dispersed carrier battle group to see the composite radar threat map seen by all the radar sensors of the entire battle group, not just the threat as seen from its own radars. It also permits vessels to launch missiles toward any threat within range of its weapons, whether or not its own sensors are tracking it. This capability would greatly extend the defensive perimeter of the task force, while providing defense in depth for exposed ships on the periphery of the task force. Initial testing of a few such ship-to-ship links showed considerable promise. The Navy plans to extend the CEC concept to include radar data acquired by patrolling Navy E-2C surveillance aircraft.

Skeptics of the RMA suggest that the CEC represents only a small piece of the total "system of systems" capability the RMA envisions. They point to shortfalls in other areas such as the inability of U.S. forces to locate and target Iraq's mobile SCUD launchers before, during, and after launches during the Gulf War; the failure of U.S. intelligence to forecast the Indian nuclear tests and the North Korean missile launch over Japan's territory; the failed effort to kill Osama Bin Laden in his encampment in Afghanistan; and the regular failures in development programs for U.S. theater ballistic missile defenses. In the following sections we will assess several of the obstacles that skeptics see to achieving the RMA. We will also assess the status and prospects for the RMA's successful development and implementation.

Possible Obstacles to Achieving the RMA

There are a number of potential obstacles to overcome in the effort to create the envisioned RMA capabilities. First, parts of the RMA may simply be technologically infeasible. Second, even if all of the parts are ultimately shown to be feasible, their integration into a seamless "system of systems" is a most formidable challenge, one unlike anything accomplished to date. Third, the RMA originated as a "top-down" concept, one strongly supported at the highest levels of the military chain of command; as such it has been subjected to scant peer review and analysis of potential vulnerabilities. Fourth, for mission success, the RMA is critically dependent on the successful completion of a long sequence of events, each step of which must be carried out in timely fashion. This sequential dependence means that, if an enemy can briefly interrupt the chain at any point, the mission may fail, and the mission must begin again from the starting point. Finally, the RMA is uniquely vulnerable to certain massive disruptions. We will consider each of these in turn.

Technological Infeasibility

Consider for a moment the main feature of the RMA component comprised of "Intelligence, Surveillance and Reconnaissance" (ISR). The main requirement of ISR is to be able to identify and classify all threats on a 200 mile by 200 mile battlefield, and continuously track their positions (as well as those of friendly forces, and non-belligerents) regardless of terrain, weather, and camouflage, to an accuracy of 10 centimeters. We are nowhere near able to do this today. Many U.S.

casualties during the 100-hour ground campaign in the Persian Gulf War were self-inflicted by other U.S. units.

A 1999 article describing impending advances in U.S. radar technologies notes that “the capability to see through foliage should be realized within 5 to 10 years.”[4] Of course, the same projection for this technology was made by the technical community as far back as the late stages of the Vietnam War and at regular intervals thereafter, especially more recently in conjunction with the “war on drugs.” A cynic might suggest that some advanced capabilities seem perpetually “just around the corner.”

Today’s reality, however, is that we have few capabilities that can locate and thereafter continuously track anything mobile to an accuracy of 10 centimeters even under ideal viewing conditions. An article in *Technology Review* on digital terrain mapping notes that a simple digital model of the earth at one meter resolution would require more than 10exp15 bytes of information, “still outside the capabilities of today’s computers.”[5] The article goes on to note the U.S. military’s interest in such a system, adding “That goal is far off….” In fact, our capabilities to find and target mobile systems are barely improved over those available to U.S. forces during the Gulf War, when the U.S. military was shown to be incapable of dealing with night-time launches of SCUD mobile missiles from the relatively flat and uncluttered desert reaches of southwestern Iraq.

One of the newer technologies brought to bear during the Gulf War was the Joint Surveillance Target Attack Radar System (JSTARS), an airborne radar system designed to detect and track moving targets on the ground. Although the JSTARS program was only in advanced development at the time of the Gulf War, it worked quite well in the relatively flat desert terrain of Kuwait and southern Iraq. However, when brought to the Adriatic area to monitor Serbian force movements in the former Yugoslavia, its performance suffered from the effects of vegetation and terrain masking in the mountainous areas of Bosnia and Croatia.[6] Moreover, because JSTARS is based on the venerable Boeing 707 airframe, it is vulnerable to both surface to air missiles and enemy fighters. This requires it to operate well to the rear of potential threats, thus reducing its effective detection and tracking range. While similar technologies might be usable on less vulnerable airborne platforms such as stealthy remotely piloted vehicles (RPVs), the U.S. track record in the development of such platforms is mixed. One once-promising RPV candidate, called “Darkstar,” was recently canceled by the Department of Defense.

Many of the same inadequacies of current technologies are evident in the other two components of the RMA: Command, Control, Communications, Computers, and Intelligence (C4I), and Precision Force (PF). For example, a study conducted by the National Academy of Sciences/ National Research Council in 1995 concluded that an enemy could readily and cheaply jam GPS signals over its territory using small, scatterable jammers.[7] The study group estimated that these small jammers could be produced in quantity for less than $100 each, and that each jammer could prevent reception of GPS signals over an area of a few dozen square miles. Joint Direct Attack Munitions (JDAMs), a major new class of inexpensive precision aircraft-delivered munitions now under development, rely on GPS signals for their precision terminal guidance. Therefore, an enemy's ability to jam GPS signals over its own territory would render these new munitions far less effective than is advertised by DoD.

Integration Into a "System of Systems" Will Be Difficult

The most formidable challenge for the RMA lies not in the development and production of individual technologies for the component parts of the RMA, but rather the combining of all of the disparate elements into a "system of systems" architecture. This "system of systems" architecture must seamlessly integrate data streams from multiple sources presented in many different formats, and do so without either losing or double-counting important data. For example, the *FY98 Report* by the Director of Operational Test and Evaluation on the Cooperative Engagement Capability notes that, "Serious deficiencies were observed during the at-sea integration testing that was conducted in early 1998 in preparation for the formal OT."[8] The report goes on to state that, "Deficiencies were in the areas of track management, net operations, cooperative engagement, engagement support, composite identification, and link interoperability."[9] As a result of these early tests, the Navy's operational evaluation of CEC and a decision to begin production have both been postponed for 2 years.

Many U.S. intelligence and other sensor systems are already producing more data than can be analyzed in near-real time by existing methods, so quantum increases in the capability for automated data recognition and analysis will be needed.

Finally, the RMA's stated intent to provide "infinite bandwidth on demand" to any user amounts only to a guarantee that any individual user (and all users collectively) can be inundated with data. But, even if all of the technology items were feasible, that does not solve the problem of providing to each user in timely fashion the precise information needed for successful completion of an assigned mission. Anyone who has spent time searching the internet looking for information will recognize the problem of receiving a torrent of data and having to spend entirely too much time trying to determine whether that mass of data contains useful information to be extracted.

The RMA proposes to solve this dilemma by postulating the existence of "intelligent agents," a network of digital helpers that will identify the critical information needed by each of the many actors, sift through masses of data to find that specific information, format it properly for human recognition and decision, and forward that critical information with highest priority to the locations where it is needed. This is to be the job of "artificial intelligence," a computer science discipline dating from the early 1970s. Unfortunately, major advances in artificial intelligence, like radar that can see through the jungle canopy, seem always to be "just around the corner." Given its track record to date, artificial intelligence capabilities adequate to solve this fundamental RMA deficiency probably lie around more than one corner.

Even if the development of "intelligent agents" were to succeed, there remains the human factors issue of establishing sufficient trust by users—the military commanders—in a largely-automated system for applying military power. Military organizations are conservative by nature, tending to rely strongly on the "battle-tested," rather than on new, supposedly "innovative," systems, technologies, and procedures, particularly when the latter are produced from computerized "black boxes" designed by civilian "outsiders." In the military context, who (or what) will persuade senior uniformed leaders that a radical new RMA system will permit much smaller forces to do the work formerly done by armies or divisions? Mere field tests and demonstrations are unlikely to be a convincing substitute for the lessons taught by "real combat experience." Moreover, today's military leaders see additional force reductions as one of their gravest military threats. Taken together, these two reinforcing factors will probably ensure strong resistance by the military to the piecemeal adoption of RMA-like capabilities as they are developed.

Little or No "Red Teaming" of the RMA Concept

The term "Revolution in Military Affairs" actually originated in the professional military writings of Soviet military officers in the late stages of the Cold War. The current version of the U.S. military's RMA originated as the brainchild of a small, computer-literate group of high-ranking military officers, together with a few DoD civilians, in the Pentagon in the early 1990s. Through their forceful advocacy, the RMA became a "top-down" program imposed on the services from the highest levels. This high-level support was crucial to the initial survival of the concept, but it has had one serious side-effect. The high-level interest and support has diminished criticism of the concept from lower echelons, and has discouraged exploration of possible vulnerabilities. (After all, a junior officer's promotion chances are not likely to be enhanced by his arguing that “the Emperor has no clothes.”)

This “top-down” process is in marked contrast to the normal weapons acquisition process in which new programs become “fair game” for analysis of potential weaknesses not only by other elements of the service proposing the program, but also by other military services who seek to prevent budget shifts across service lines and by a host of defense analysts at think-tanks and non-governmental organizations. This process fosters a healthy debate and searching analysis of possible weaknesses well before a program has reached the point where it becomes “unstoppable.” Even after this point is reached, for major programs which require large budget expenditures, DoD often creates a separate group, called a “Red Team” to try to devise new and novel ways an enemy could counter the proposed new capabilities.

For example, in the early days of the Air Force’s program to apply “stealth” characteristics to new combat aircraft, Congress directed the Defense Department to create a Red Team. The job of this Red Team was to search for potential systems and techniques to defeat the expected signature reductions that stealthy aircraft would produce. Since the methods of producing stealth are closely guarded secrets, the DoD initially limited membership on the Red Team to Air Force officers with requisite clearances. Congress, however, insisted that Red Team membership be broadened to include members of other military services as well. Despite the stealth Red Team’s best efforts, no new and novel methods of defeating stealth technology were discovered, and the real-world performance of the Air Force’s F-117 and B-2 aircraft have been amply proven in the skies over Baghdad and Belgrade.

As the above example makes plain, a Red Team will not necessarily discover fatal flaws in a new concept. But in the absence of a Red Team, such flaws are unlikely to be discovered. There is today no U.S. Red Team searching diligently for possible enemy counters to the capabilities of the RMA.

Possible Counters to the RMA: Momentary Interruptions

In this section we will consider a few possibilities for a clever enemy to diminish the capabilities of the RMA. One possibility stems from the fact that the successful completion of any mission conducted under the RMA requires the successful completion of each and every step in a sequence of steps. To provide a concrete example, let us consider the effects of the introduction of stealth characteristics on the air defense mission.

Stealthy aircraft are not invisible to radar. Their current combat edge stems instead from their ability to disrupt a lengthy chain of events that an air defense system must complete both successfully and in timely fashion to destroy an intruding aircraft. The air defense system must first use long-range radar systems to detect an approaching aircraft at considerable range. This detection provides the time to bring to bear either interceptor aircraft or activate surface-to-air missile (SAM) sites to shoot down the intruder. Second, the long-range radar must continue to track the invading aircraft while guiding an interceptor aircraft or alerting a SAM battery as to the progress of the intruder. Third, when the intruder approaches a SAM site, or when an interceptor aircraft converges on an intruder, that defender must independently detect, and then track, the intruder until it is in a position to bring its weapons to bear on the intruder. This is not easy, because stealth tends to reduce both SAM and interceptor radar ranges to a greater degree than long-range search radars. Moreover, the intruder will be able to detect the location of interceptor and SAM site radars from their emanations long before those systems can detect it. Thus, the intruder can maneuver to try to evade radar detection by the defenses. Finally, the terminal homing system in the SAM or air-launched missile must function to detonate the warhead within the lethal range against the particular intruder.

What stealth does for the intruder is to greatly reduce the range at which various radars used by the defense system can detect and track it. By reducing the range at which the long-range radars can detect a stealthy intruder, stealth minimizes the reaction time for the defenses to send interceptors to find it. Because stealth greatly reduces the detection range for SAM radars, a defense system that against conventional intruders provides multiple overlapping SAM coverage in depth now has holes in its coverage through which stealthy aircraft can slip. Although interceptor aircraft are very mobile, their physical size limits the power of their self-contained search radar; they therefore have great difficulty independently detecting and tracking a stealthy intruder, even though a long-range radar may still be tracking it. Finally, even if an interceptor were to find itself in position to engage an intruder, there are many forms of interceptor missile warhead fusing that would be baffled by the small signature of the stealthy intruder, and might fail to function effectively.

In short, stealth works, not just in laboratories and on test ranges, but in the real world against real enemy defenses. It works not by conferring invisibility or invulnerability, but by diminishing the performance and reaction times of complex air defense systems. This greatly reduces the probability that an entire chain of events, all of which must be successfully performed to shoot down a stealthy aircraft, can in fact be successfully achieved.

What is the relevance of this discussion of stealth for the RMA? Consider the complexity of operations assumed to occur under the RMA. Each specific offensive strike mission conducted under the RMA must perform a sequence of activities both flawlessly and on tight time-lines; any disruptions or delays in the processing and transfer of information are likely to lead to mission failure. Potential enemy targets must be detected by one or more sensors and thereafter tracked continuously. The location of these targets must be forwarded to a command center, where the data must be integrated with similar target data from other sensors, to form an integrated view of the battlefield. Some kind of artificial intelligence network must analyze this mass of situational data and establish priorities among targets to be attacked. The network must also be aware of the availability, range, and warhead types of all of the offensive force's strike weapons, so as to prioritize the application of the most effective weapons against the most important enemy targets. Then, the artificial intelligence machine must issue orders to all firing units, assigning individual weapons to be fired to specific enemy targets, and assigning specific launch times to each, to insure efficient arrival "times on target" to avoid causing fratricide among incoming weapons. Finally, each individual firing unit must be given the latest updated coordinates of each assigned target just prior to a weapon launch, either directly from the sensor(s) tracking the target, or from the command center.

It is clear that the complex and highly interactive process described above would be vulnerable to disruptions of data flows. It is likely that, for any single mission, even modest interruptions of sensor or communications links, perhaps even only a momentary outage, could produce a "reset"—could require the cycle of target detection and tracking, data integration, optimization, and target assignment to start over. To achieve mission success, the RMA must successfully carry out a lengthy sequence of steps, where, even if each step in the chain has a high probability of success, the overall probability of success may not be that high. For example, if mission success requires the successful completion of five sequential steps, where the probability of success of each individual step is *p*, then the cumulative success probability if *p* = 0.9 is less than 60 percent. For lesser probabilities of success (*p*) for each individual step, the overall mission success declines precipitously. For example, if *p* = 0.8, it is only one in three; for *p* = 0.5, it is only 3 in 100; for *p* =0.3, it is only 2 in 1,000.

In sum, stealth constitutes a "robust" way of achieving high mission effectiveness. To defeat stealth, enemy air defenses face a "hard to satisfy" requirement to successfully carry out each step in a long sequence of "low-probability-of-success" steps. In contrast, the RMA appears to propose to achieve its effectiveness in a "tenuous" way, or at least an "exacting" way, by requiring the successful completion of each of a lengthy sequence of steps. For this mission success to occur consistently, all of the individual probabilities of success for each step must be extraordinarily high.

Of course, none of these considerations pose a difficulty for the RMA's "true believers"—such problems are simply assumed away by the RMA's postulations of "continuous and complete target identification and tracking," "infinite bandwidth on demand," and the construction of a flawless "system of systems."

How might "momentary disruptions" arise? The military is critically dependent on two technologies for communications—interconnected digital communications using commercial circuits and networks and wireless communications for the transmission of orders to field units. This encompasses both the use of commercial telephone lines and satellites for long-haul communications and field radios for shorter or line-of-sight communications. Most combat equipment, whether on land, sea, or in the air cannot be hard-wired to dedicated, high-capacity lines. Both provide opportunities for disruption of the RMA.

Already today, more than 95 percent of DoD's worldwide communications travel over commercial networks. This constitutes both a new advantage and a new vulnerability for our military forces. It is an advantage in that the military has a far wider range of communications networks available for its use, and its costs are much lower than if it had continued to design, build, and use its own dedicated networks. It is a disadvantage, however, since, as Director of Central Intelligence George Tenet observed, "We share the same networks as our adversaries."[10]

Moreover, much of the commercial infrastructure is privately-owned and operated, and may be vulnerable to disruption. The most likely avenue for attack is that called “information warfare.” Information warfare is a method of attacking an enemy by seeking to disrupt his communications and other vital parts of his infrastructure by penetrating his digital networks and destroying or altering computer codes that control the network’s functions and data streams. DoD has an agency that regularly launches computer attacks against other DoD components; in these tests, the attacking agency succeeds in breaking in on about two of every three attempts, and, worse yet, far less than ten percent of the system operators even recognize that their system was breached.[11]

Deputy Secretary of Defense John Hamre has declared that the Pentagon is already “under attack” from computer hackers whose identities, nationalities, and locations are undetermined. This situation is exacerbated by the fact that today’s leaders, civilian and military, are the product of both their knowledge and their environment. In the military, as in the corporate world, most of today’s leaders grew up in a planning environment dominated by large mainframe computer management systems, the security of which was assured by physical isolation and barriers. These military and corporate leaders have little intuitive feel for the new perils of the PC and the network world.

As a result, in the military world, while concerns about information security are rising, the resources necessary to begin to cope more effectively have not been requested. The perils are even worse in the civilian sector on which the military increasingly relies. Most corporations, including those that own and/or run most of America’s vital infrastructure systems, are spending far too little on information security measures to defend against the new perils of break-ins by hackers, disgruntled employees, competitors, and/or foreign intelligence services.[12]

Possible Counters to the RMA: Massive Disruption

The final scenario of RMA vulnerability we will examine is the degradation of effectiveness of the RMA that could be caused by an enemy possessing even a single primitive nuclear weapon and a ballistic missile capable of lofting it to an altitude of a few tens to a few hundreds of kilometers above its own territory. A nuclear detonation at such an altitude would produce a massive high-altitude electromagnetic pulse (HEMP),[13] which can be thought of as a broad-band radio wave that is millions of times more powerful than an ordinary radio broadcast.

HEMP effects were first discovered by U.S. scientists during a series of atmospheric nuclear tests over Johnston Island in the Pacific in 1962. The test in question, although conducted more than 800 miles from Hawaii, disrupted telephone switch gear and the electric power network, blew out streetlights, and disrupted radio broadcasts throughout the Hawaiian Islands. It also caused the failure of several satellites which passed through a region of residual charged particles left as debris from the nuclear detonation. Since this unintended "experiment," scientists have learned much more about HEMP effects on electronic equipment, both in spacecraft and in systems on the ground.

The HEMP threat was a serious concern to U.S. (and probably Soviet) defense planners throughout the Cold War, because of the huge nuclear arsenals on both sides. The Cold War solution to the HEMP threat involved both the shielding of certain electronic components inside EMP-resistant enclosures, and the use of specially-designed and -produced radiation-hardened electronic chips. The last military satellite system to be so equipped is the Milstar series of satellites now on orbit. However, in the past two decades, the demand for large-scale integrated circuits for civil uses has swamped military demand. Chip manufacturers are no longer interested in the design or production of special radiation-hardened chips (or in putting up with what they consider oppressive DoD acquisition regulations and bureaucratic procedures). In addition, the military budget has declined too far and is stretched too thin to support special-purpose chip manufacture and hardened, dedicated military communications satellite networks.

A side effect of Milstar's hardening against HEMP effects is that the resulting system has greatly-reduced data transmission rates. Milstar's planned role in a nuclear war was simply to ensure that the relatively short nuclear release message from the National Command Authorities to the nuclear-armed forces in the field could be transmitted with very high confidence.

HEMP effects would be most immediately felt by satellites within line-of-sight of the nuclear detonation, which is to say, roughly half of all satellites on orbit. Moreover, satellites operating at medium altitudes would encounter cumulative EMP effects as their orbits bring them through the residual radiation region surrounding the nuclear detonation point. To illustrate, if Iraq were to detonate such a weapon, more than half of the geostationary satellites would cease to function, including weather, missile warning, and communications satellites. Civilian as well as military satellites (except for Milstar) would be knocked out of action. So too would all of the GPS satellites on Iraq's side of the earth, along with all of the intelligence sensors of all countries on Iraq's side of the globe. Moreover, all of the lower-altitude commercial satellites such as Iridium and the GPS satellites initially shielded by the earth would cease functioning after only a few revolutions.

While these effects on spacecraft are far-reaching, the effects on the ground under and around the point of detonation would also be devastating, since enormous electric currents are generated in wires, antennae, fences, and metal structures. Where such conductors enter buildings and vehicles, a pathway exists for the HEMP to penetrate vulnerable systems. Electronic systems connected to such conductors can suffer extreme damage. Worse yet, the increased packing density of large scale integrated devices such as computer chips makes them increasingly vulnerable to burnout from even small voltage spikes.

Since an enemy willing to use this technique would control the time of detonation, it could shelter and/or turn off much of its own sensitive electronic equipment. But the real point is that a potential aggressor is far less dependent on high-tech electronics than is the United States. While such a detonation might cut off the aggressor's nose, it could decapitate much of today's high-tech U.S. battlefield forces.[14]

On The Military Utility of the RMA

To this point, this chapter has focused on impediments to the achievement of the RMA. We now shift focus slightly to explore what kinds of military contingencies would benefit most from a fully-developed RMA capability.

Large-Scale Maneuver Warfare

The 1991 Persian Gulf War clearly established the substantial superiority of U.S. equipment, tactics, situational awareness, and leadership and training over what was regarded at that time as the third or fourth best army in the world. Since that drubbing, Iraq's military has shown no inclination to further challenge U.S. or Kuwaiti forces, and the United States has demonstrated the capability to destroy fixed installations anywhere in Iraq with total impunity, using a mix of cruise missiles and manned aircraft.

This strongly suggests that, given enough time and places to marshal its forces, current U.S. conventional military forces are capable of repulsing the military forces of any Third World power which sought to invade and capture by force the territory of a U.S. ally or friend. This is a statement of capability, not necessarily intent, but potential enemies everywhere have noted the results of the Gulf War.

It is important to note the caveat "given enough time and places to marshal its forces." In the Gulf War, it took the United States and its allies more than a month to bring enough forces into the region to be confident of stopping a further Iraqi thrust into Saudi Arabia, and a full six months to establish both the forces and the supply lines needed to expel Iraqi forces from Kuwait. Both those forces and the necessary supply lines have since been withdrawn from the region, which has necessitated a substantial and expensive buildup of forces each time Saddam Hussein has threatened to abrogate the UN mandates imposed on Iraq at the conclusion of the Gulf War.

This raises two questions. Could the RMA provide a sufficiently rapid-reacting capability that it could stop an enemy's short-warning invasion of the territory of a friend or ally? If not, could the RMA provide a more rapid-reacting military response capability than the current extensive (and expensive) system of marshaling expeditionary forces and extending their supply lines?

The proponents of the RMA would surely argue "Yes" to the latter. Some might even answer both affirmatively. But when we consider that the CIA was still projecting that Iraq would not invade Kuwait on the eve of the invasion, as well as that the Saudi government did not grant permission for U.S. forces to reinforce the Saudi military until three days after Kuwait had fallen, the latter somewhat strains credulity.

While the RMA envisions the use of fewer U.S. troops on the ground than are assigned to current armored and mechanized units, this is based on the implicit assumption that those smaller U.S. forces will be *in place* at the start of an enemy invasion and will survive by attriting the advancing enemy forces from a vantage point well outside the range of enemy fire. Thus, the RMA also implicitly assumes that all the necessary surveillance and reconnaissance assets to maintain exacting surveillance of a battlefield are in place and operating when the enemy invasion begins. Satellite-based systems are "in place," of course, and some long-range aircraft could arrive within hours, but many other assets such as RPVs and their support and control systems would have to be transported to the theater and then made operational.

A tenet of the RMA asserts that weapons platforms are increasingly irrelevant. This assertion spares RMA proponents from having to explain exactly how all of the precision strike systems—most of which have far less than intercontinental range—just happen to be located in the proper theater when an enemy attack begins. If they are not, then the United States faces much the same kind of deployment problem that it faces today.

Reducing the numbers of deployed troops would reduce the volume of personnel-related resupply items significantly, but the limiting factors for high-intensity warfare are still the ability to resupply both fuel (or, POL, in military jargon) and munitions. Such was the thirst of the allied air forces during the Gulf War that, by the end of the first week of the air war, the Kingdom of Saudi Arabia, sitting atop the largest petroleum reserves in the world, had become a net importer of POL, a situation that continued throughout the air war and the 100 hours of ground combat.

The American public has grown accustomed since the Gulf War to pictures of cruise missiles arcing up from U.S. warships, on their way to various targets guided by signals from the GPS satellites. What most do not appreciate is that the supply of these cruise missiles aboard an individual ship is limited, typically a few dozen weapons. When fired, they are gone. Their replacement requires the warship to return to a port to be resupplied. Moreover, most sea-launched cruise missiles are given a pre-determined target point at the time of launch and cannot be retargeted in flight. This makes them unsuitable for attacking mobile targets that can move away during the cruise missile’s time of flight. Finally, reliance on cruise missiles is an expensive proposition, one affordable only for small attacks. Each Navy cruise missile costs about $750,000, a one-shot cost to deliver a few hundred pounds of high explosive to a fixed point. To stop an enemy armored incursion relying on cruise missiles alone could require many thousands, an investment the United States is unlikely to have made in advance of a major conflict.

This high cost is one reason that DoD is developing a program called the Joint Direct Attack Munitions (JDAM), a set of guidance kits to attach to conventional unguided bombs carried by manned aircraft that will steer the bombs after release to an aim point, using GPS satellites for navigation. Each JDAM kit is expected to cost less than $50,000. The kits can be used on a wide range of existing bombs of up to 2,000 pounds of high explosives. Released from high altitude, JDAM-equipped bombs can glide for several tens of miles, allowing a manned aircraft to release its weapons well away from local air defense systems. These weapons require that GPS satellites be operating and that their signals not be jammed.

In addition to cruise missiles, the other weapon system of choice early in a conflict is stealth aircraft. In the 1999 air attacks against the former Yugoslavia, two U.S. B-2 stealth bombers each released 16 prototype JDAM 2000-pound bombs in the first use of both the B-2 and the JDAM in conflict. While each B-2 puts at risk a crew of only two, and with aerial refueling has a global non-stop range, there will only be 21 B-2 bombers. Thus, even a full surge effort would only deliver 336 JDAM weapons. Meanwhile, the F-117 stealth fighter carries only two bombs and was also procured in limited numbers. The total F-117 force can deliver only a few more than 100 weapons per surge.

In the end, because we did not buy more than a token force of the relatively invulnerable, long-range stealth bombers, we will continue to have to use large numbers of non-stealthy, short-range tactical aircraft to deliver massive precision firepower against an invading force. These systems must be deployed to a theater of operations where they will be critically dependent for sustained operations on our ability to rapidly establish resupply lines for both POL and munitions, as well as on the timely deployment of a host of supporting aircraft to suppress enemy defenses, provide battlefield surveillance, and thwart enemy aircraft. Each of these in turn will have its own special resupply needs.

How long does it take to deploy forces and establish re-supply lines? It depends on the distance from the United States, on the availability of en-route bases owned by friendly third parties, on the distance by sea of the theater from U.S. ports, on the availability of indigenous labor and transport from the foreign port to the U.S. bases of operations in the theater, and on a host of other factors. Most resupply comes by sea since there isn't enough airlift capacity to resupply a sizable ground and tactical air force in a theater of operations. If the impending conflict is an ocean or more away, the first availability of sealift resupply will be nearly a month after a decision to activate the sealift vessels. The track record for our intelligence services providing a warning of conflict a month or more in advance is dismal. Even if they could do so, our military and political leadership may be reluctant to undertake the necessary actions in timely fashion.

Thus, absent revolutions in both intelligence and top-level decision-making, the RMA is unlikely to fundamentally alter the response options for cases where the United States is forced to respond to a *fait accompli* in some distant land. Here, we must play “catch-up ball” for days to weeks before we have in place the forces and supply lines necessary to prevail. The RMA may reduce the overall troop levels required, but it does not appear to eliminate the need for substantial deployments of weapons delivery systems to a theater of operations or the establishment of a large resupply effort to permit sustained operations for whatever period is necessary to dislodge enemy forces.

“Hostage” Scenarios

A related issue is whether the RMA would be useful in “hostage” scenarios. By hostage scenario, we mean a situation in which an enemy force threatens to capture (or has already captured) some territory of extraordinary value and threatens to destroy it if attacked. The Iraqi invasion of Kuwait was such a situation. Iraq’s forces captured Kuwait’s oil fields and oil export facilities, set explosive devices around all of them, and threatened to blow them up if the West tried to dislodge them. This failed to be a big enough hostage to dissuade the coalition of forces from attacking and dislodging Iraqi troops, even though this resulted in the destruction of the oil facilities and required some two years to put out the fires and repair the damages.

The main reason for the failure was that the world’s largest economies were still deep in recession or just recovering, so the loss of Kuwait’s and Iraq’s oil did not cause supply problems. But suppose Iraq had not stopped at Kuwait’s border with Saudi Arabia? It seems clear that Iraq could have captured much of Saudi

Arabia’s oil production and export facilities as well as Kuwait’s. Now, a threat to put all of it to the torch would have had teeth. Had Iraq had an ounce of diplomacy, it could also have guaranteed free flow of oil so long as it were not attacked. If all of Kuwait’s and Iraq’s oil exports and the lion’s share of Saudi oil had been lost in 1991, the economic effects on Western economies would have been severe.

Whether this could have prevented the emergence of the coalition, and whether the United States would have tried unilaterally to expel Iraqi forces, is sheer speculation. The same sustained bombing campaign and the same massive U.S. ground forces would ultimately have expelled the Iraqis from both Saudi and Kuwaiti territory. But, it seems clear that such a hostage scenario would have presented many more problems for U.S. leadership.

Could the RMA help solve this kind of scenario, either by preventing the initial *fait accompli* from occurring, or by rescuing the “hostage” from being “shot” during the expulsion of the enemy force? Given the analysis above, it seems unlikely.

Asymmetric Warfare

What about scenarios of conflict other than stopping or expelling an invading armored force? The concept of asymmetric warfare has been postulated as a more likely form of conflict that might be used by an enemy than a massive invasion of the territory of a friend or ally of the U.S. “Asymmetric” conveys the appreciation by an enemy that it cannot prevail in a head-to-head battle with U.S. forces, and therefore must find alternative methods of conflict to deter or defeat U.S.

capabilities and actions. Proposed asymmetric capabilities encompass guerrilla warfare, urban warfare, terrorism, and information warfare.

Consider guerrilla warfare, particularly urban guerrilla warfare. Neither U.S. forces in Vietnam and Somalia nor other highly-regarded military forces—Russian forces in Afghanistan and Chechnya, Chinese in Vietnam, and the British in Northern Ireland—have distinguished themselves in this kind of fighting. The essence of guerrilla warfare is an enemy that at times of its choosing is largely indistinguishable from a civilian populace and that relies primarily on hit-and-run tactics and the steady infliction of casualties on a superior force. What might the RMA contribute to U.S. forces engaged in such conflicts?

It is safe to suggest that the ISR capabilities of the RMA will not be able to distinguish between civilian noncombatants and military irregulars when they are intermixed, especially in urban warfare. In densely populated areas like cities, the ISR will not be capable of maintaining continuous track of individual vehicles or people, as urban buildings create “canyons” that continually interrupt coverage from any sensor location other than “directly overhead.” As both the Chechen resistance and the U.S. mission to Somalia showed in Mogadishu, local knowledge of urban terrain gives an enormous advantage to urban guerrillas operating against an occupying military force. The RMA’s indirect fire will almost certainly produce widespread civilian casualties if employed against urban areas.

The guerrilla’s usual battle plan is to avoid direct engagements with enemy units with superior firepower. Instead, guerrillas rely on hit-and-run attacks, boobytraps, car bombs, and the like, trying to inflict over time an unacceptable level of casualties on the enemy to compel withdrawal. This happened rapidly to the United States in Somalia, thanks to the “CNN effect,” and more slowly to the Russians during their 1994-96 occupation of Chechnya since Russia had no CNN to bring the war home to its citizens. The RMA does not appear to provide new ways of driving guerrillas from urban areas, so it would appear that ground troops would still be needed. The military’s heavy weapons are generally ill-suited to urban conflict and often vulnerable to attack from above from buildings fronting on streets.

Terrorism can also be a way for an enemy to open a “second front” against our homeland, against those of our friends and allies, or against some nodes upon which we depend to continue a military campaign. It can take many forms and assume many levels of violence. When directed against the United States, its intent would be to force a U.S. withdrawal from an arena where it enjoys a military advantage by exploiting U.S. weaknesses in other areas.

U.S. citizens are not likely to remain immune either while traveling abroad or even at home. Indeed, there is growing concern about the possibility of terrorist attacks against U.S. metropolitan areas via weapons of mass destruction—chemical, biological, radiological, or nuclear weapons. It is difficult to project whether mass civilian casualties at home would strengthen or weaken U.S. resolve for continuing a conflict in a remote area. In any event, it is difficult to develop prompt and convincing evidence of a particular foreign power’s complicity in a terrorist attack. The RMA does not appear to offer much to the long-term struggle against terrorism, although ISR assets might play a role in improving surveillance.

“Ethnic Cleansing”

The limited success of NATO’s 1999 bombing campaign to compel Serbia to negotiate a peaceful settlement in Kosovo and to stop expelling or killing ethnic Albanian residents of Kosovo provided a perfect scenario to highlight the RMA’s hoped-for capabilities. However, much of the displacement of Kosovars and many of the atrocities were the work of paramilitary organizations rather than the uniformed Serb military. Even if NATO had better means to attack Serb tanks and artillery, it is not clear that this would have seriously impeded the reign of terror that drove the flood of refugees out of Kosovo. The RMA may have made the Serbs more cautious about blatant use of tanks and artillery, but it was not of much help in distinguishing between a thug and a refugee. Thus, in situations of ethnic conflict where one side has a preponderance of power and the other is effectively unarmed, the RMA has yet to prove its worth.

Finally, RMA proponents seem not to have considered likely counter-moves by opponents. Suppose in response to NATO’s initiation of use of its RMA capabilities, the Serbs on a large scale used Kosovars as “human shields” for their forces. Then what?

Conclusions

The RMA is a “Made in America” concept, the U.S. vision of a “perfect war” capability—the perfectionist application of precisely measured force to defeat an enemy rapidly, thoroughly, and completely, with no U.S. troops placed at risk and no U.S. casualties.

Wouldn't that be wonderful? But the reality is different, and is likely to be different for a long time. Indeed, the RMA can be summed up in a line from a Robert Frost poem:

> *The woods are lovely, dark and deep,*
> *But I have promises to keep,*
> *And miles to go before I sleep.*[15]

[1] As will be explained below, a U.S. failure at any single point in the chain results in mission failure. Under such a structure, the enemy need only focus on causing random, temporary disruptions to a few parts of such a "system of systems" to cause widespread mission failures.

[2] "America's Information Edge," Joseph S. Nye, Jr. and William A. Owens, *Foreign Affairs*, March/April 1996, also reprinted as Chapter 4 of Volume II of *The Information Age Anthology: National Security Implications of the Information Age*.

[3] Author's personal notes from hearing.

[4] David A. Fulgham, "New Radars Peel Veil From Hidden Targets," *Aviation Week & Space Technology*, January 18, 1999.

[5] "Think Globally, Act Digitally," *Technology Review*, (March/April 1999), p. 25.

[6] See "Report, FY 98," Director, Operational Test and Evaluation, Department of Defense, Feb. 1999, pp. V-104-106.

[7] "The Global Positioning System: A Shared National Asset," National Research Council, National Academy Press, Washington, DC, 1995.

[8] "Report FY 98," *op. cit.*, p. IV-32.

[9] "Information Security: Risks, Opportunities, and the Bottom Line," 1998 Sam Nunn NationsBank Policy Forum, Georgia Institute of Technology, Atlanta, GA, 1998, p. 9.

[10] Ibid., p. 8.

[11] See *The Report of The Presidential Commission on Critical Infrastructure Protection* (Washington, DC: U.S. Government Printing Office, 1997).

[12] A full discussion of the information warfare threat is beyond the scope of this chapter, but the vulnerability is real. For discussions of various types of threats, see Chapters 7 through 13 of Volume II of *The Information Age Anthology: National Security Implications of the Information Age*.

[13] A more technical discussion of this phenomenon can be found in Samuel Glasstone, ed., *The Effects of Nuclear Weapons*, (Washington, DC: U.S. Department of Defense, 1964).

[14] For a more complete discussion of this risk, see, e.g., Sean J. A. Edwards, “The Threat of High Altitude Electromagnetic Pulse to Force XXI,” *National Security Studies Quarterly*, (Autumn 1997).

[15] Robert Frost, “Stopping By Woods On A Snowy Evening,” 1923.

PART FOUR

INTRODUCTION

What will war in the Information Age be like, and how will it be fought? This is the fundamental question with which military planners and strategists are grappling. The five articles in this section offer widely different answers. None examines large-scale conflict between the United States and a peer competitor since no peer competitor currently exists or can be foreseen in the near or mid-term future.

The first article paints a picture of how several regional powers may use asymmetric warfare to take on the United States. The second offers an assessment of how sub-state actors may employ and are employing information technology to pursue ends which conflict with the objectives of the United States and other great powers. The last three provide analyses of what went right and wrong with information warfare and information operations in three conflicts in the 1990s—Somalia, Bosnia, and Kosovo.

“A Failure of Vision Retrospective,” co-authored by Fred Kennedy, Rory Welch, and Bryon Fessler, presents a chilling early 21st century scenario in which regional powers launch a three-pronged attack against the United States. All three prongs emanate from unidentified and unidentifiable sources, precluding an American ability to respond.

The first assault is biological. Using advanced global positioning capabilities, a single pilotless plane is used to initiate an anthrax epidemic in Washington, D.C., that decapitates the American government. The second assault takes advantage of U.S. dependence on satellites for communications and data transmission, the limited U.S. ability to defend those satellites, and the lack of back-up systems for many of these space-based assets. Following the stealthy destruction of many satellites, not all of which were American or Western, confusion is maximized by a third assault, the initiation of a virus-driven information warfare attack against the Western information infrastructure.

Unsure of who launched the attacks or what the objectives of the attacks are, the United States, in the authors' scenario, is unable to respond. The United States is far from defeated, but American military might and economic capabilities are nevertheless weakened and U.S. will is paralyzed. Consequently the United States retreats from the position of sole global leadership it occupied since the collapse of the Soviet Union, leaving the field open for others to expand their international influence.

Could such a series of events unfold? Of course not…or, in the Information Age, could it?

The second article, "The IW Threat from Sub-State Groups: An Interdisciplinary Approach" by Andrew Rathmell et al., examines the ways in which sub-state actors are employing and may employ information warfare techniques. Concentrating on "software warfare," that is, the penetration and disruption of an opponent's computer system, the authors first discuss a number of common penetration and disruption strategies.

They next turn their attention to how sub-state actors, particularly terrorist groups may use information warfare. Noting that terrorist groups prefer to use professional hackers as opposed to amateurs to further their ends, Rathmell and his fellow authors stress two points. First, they observe, terrorist groups may well have used both the threat and reality of information attacks against commercial firms to extort funds from them, and second, the scope of such extortion is difficult to track because firms want to maintain the public image that their information bases are secure.

Rathmell et al. also provide profiles of several sub-state groups that are using the Internet, advanced communication technologies, and other Information Age technologies to oppose and in some cases try to undermine state governments. Although the authors draw striking contrasts outside the areas of information warfare between the groups on which they concentrate, three radical Islamist-oriented groups from the Persian Gulf area and the Provisional Irish Republican Army (PIRA), within IW, there are more similarities than dissimilarities. Both the loosely organized Gulf groups and the more tightly structured PIRA use information and communication technologies for consciousness-raising and propaganda operations, the authors believe that none have yet devoted their attention to IW in its broader applications.

Notably, the authors assert that the Gulf groups may be more willing to use information warfare techniques than the PIRA. The Gulf groups, they believe, are at earlier stages of their anti-government campaign than the PIRA, and may not yet understand the potential of IW. Conversely, Rathmell et al. argue, the PIRA may be constrained from wider use of information warfare by three factors. First, the authors claim that information warfare does not fit the PIRA's organizational culture and self-image. Second, the sociological background of most PIRA leaders does not fit well with IW, Rathmell and his co-authors believe. Third, the authors maintain that the PIRA's extreme emphasis on operational security steers the organization away from information warfare.

"The IW Threat from Sub-State Groups" offers four conclusions, several of which run counter to prevailing thought. First, in accord with prevailing views, it observes that a pool of personnel skilled in IW is available to do the bidding of terrorist groups if they so desire. Second, even authoritarian states such as Saudi Arabia have been unable to respond effectively to sub-state groups that have made "sophisticated use of modern communications methods." Third, Islamist opposition groups are making effective use of IW to leverage their limited resources to achieve a major impact. Finally, although the potential impact of IW attacks on Great Britain's national information infrastructure could be "highly disruptive," reasons of "organizational culture and operational security" may influence groups such as the PIRA to forego such attacks.

Rick Brennan and R. Evan Ellis, the authors of the third article in this section, "Information Warfare in Multilateral Peace Operations: A Case Study of Somalia," use a broad definition of Information Warfare and point out that it is not only the United States that conducts IW. Including the media and public relations as elements of IW, the authors argue that the United States must better learn to use effectively all types of in formation in warfare if it is to achieve its objectives. Brennan and Ellis detail both the successes and failures of the American intervention in Somalia, concluding that the absence of a national information strategy frustrated the U.S. ability to achieve its objectives in Somalia. They label this omission a “glaring deficiency.”

The authors begin by exploring the role of information operations in peace operations. They persuasively argue that in peace operations, legitimacy is the military “center of gravity.” They further assert that information warfare can be “divided into the functional areas of perception management,” information degradation or denial, and information exploitation.” Perception management, they maintain, “seeks to manage the flow of information in order to gain and maintain legitimacy.” Continuing, they posit that in military operations other than war, information degradation or denial “may seek to disrupt or contain information flows between parties to the conflict who place themselves in opposition to the peace process.” Finally, information exploitation, according to Brennan and Ellis, is the “use of information of all types to achieve strategic, operational, and tactical objectives.”

Brennan and Ellis use these definitions to structure their analysis of the U.S. and UN intervention in Somalia during the early 1990s. They reach a number of surprising conclusions. For example, they provide evidence that Somali warlord Mohammed Farah Aideed consciously employed perception management aspects of information warfare to good effect even before the United States and UN intervened, staging events, playing on the international media’s ignorance of Somalia, spreading disinformation, and engaging in other forms of agitation and propaganda. These efforts continued during the U.S. and UN intervention.

Conversely, despite its more extensive perception management capabilities, the United States never employed a national level information strategy even though it on occasion altered its military policies and practices to affect U.S. public perceptions.

As for information degradation and denial, Brennan and Ellis conclude “the relatively low-tech Somalis” were “able to define the technological intensity of the battlefield more to their own benefit.” Aideed escalated violence to cut the flow of information to UN and U.S. forces, relied on word-of-mouth communications to reduce the value of U.S. electronic information gathering capabilities, and used civilians to disguise the movement of troops and weapons. Conversely, aside from the destruction of Radio Mogadishu, U.S. information denial efforts had “little impact on the Somali warlords for a number of political and military reasons.”

The authors argue that both sides evidenced ability to exploit information despite significantly different information infrastructures and technological capabilities. Nevertheless, the United States in particular had vulnerabilities. They included the assumption that the U.S. inability to detect signal traffic meant that Somali communication had been curtailed, the U.S. inability to understand Somali culture and language, the failure of inter-service, intra-service, and intra-coalition intelligence coordination.

Brennan and Ellis use these findings to develop nine overarching lessons for information warfare in military operations other than war. The lessons include deciding upon and articulating a fully integrated military strategy that includes information operations, recognizing legitimacy as the center of gravity, refraining from identifying a single person or group as the enemy, and including public affairs and psychological operations as central components of information warfare. Other lessons are recognizing that multinational forces are especially vulnerable to opponent information warfare efforts in perception management and understanding that the lack of parallelism between U.S. information assets and those of low-tech opponents reduces U.S. capabilities to degrade an opponent's information or to deny information to him. Several of these are difficult lessons to learn, but all the authors argue, are crucial to success in military operations other than war during the Information Age.

The fourth article in this section, "Target Bosnia: Integrating Information Activities in Peace Operations" by Pascale Combelles Siegel, reaches many of the same conclusions and draws many of the same lessons that Brennan and Ellis do. In contrast to the UN and U.S. intervention in Somalia, the UN and NATO intervention in Somalia designed and implemented an information campaign designed to "seize and maintain the initiative by imparting timely and effective information within the commander's intent."

UN and NATO information efforts had three components: a public information campaign designed to "establish "NATO's credibility with the international media to gain support from the contributing nations;" a psychological operations campaign designed to "influence the local population and its leaders" to favor UN and NATO efforts; and a civil-military cooperation campaign designed to "inform audiences about civil-military cooperation and to release information to aid the local population." All three campaigns had some notable successes. Nevertheless, difficulties also developed in all three campaigns that complicated the UN's and NATO's ability to achieve their objectives.

Siegel observes that the public information (PI) campaign was directed first toward the on-the-scene international media, recognizing that the media mediates the information that reaches broader publics. This part of the PI campaign had three parts: a proactive public information policy, a free and open media access policy, and complete, accurate and timely reporting. The author reports that "most commanders gave full support to their PI teams," but that complications arose when "a sudden incident would occur and be reported in the media before [the military] was prepared to make a public statement." Other difficulties that arose included decreased levels of command support for public information operations as NATO operations replaced UN operations and different views about and operating procedures concerning PI between different countries within the UN and NATO. Nevertheless, Siegel concludes, the PI campaign was for the most part successful.

Siegel reaches a different conclusion regarding the psychological operations (PSYOP) campaign. The author attributes this to three factors. First, "political sensitivities surrounding the use of PSYOP forces made it more difficult to run an effective, multinational PSYOP campaign." Second, this led to a "weak and conciliatory" PSYOP message that had a "limited…impact on the local populations." Closely related to this, PSYOP forces had "difficulties in adapting to the local culture and media habits." Finally, the PSYOP campaign's assessment of its own efforts "was at best limited," thereby reducing the campaign's ability to modify its message to achieve greater effect.

The civil-military cooperation (CIMIC) campaign led to similarly disappointing results, Siegel argues. CIMIC activities simply did not arouse media interest, the author notes, a situation that only grew worse as new CIMIC units were rotated into theater and defined their duty as providing command information. Indeed, Siegel concludes that by 1997, CIMIC activities were "essentially invisible to the international and local publics."

At the same time, the author provides evidence that when the various aspects of the information campaign coordinated their efforts, the information campaign acted as a force multiplier for NATO commanders. Coordination proved a difficult task, however, Siegel posits that the UN's experience showed that coordination was a give-and-take process, while NATO's experience indicated that coordination depended on the commander's commitment.

When all is said and done, Siegel identifies nine lessons that may be derived from the Bosnia experience. First, PI principles and guidelines must be clearly articulated. Second, PI must be adapted to the speed of media reporting. Third, PSYOPS must be strengthened. Fourth, all information operations must be adapted to local audiences. Fifth, the three branches of information operations must be closely associated. Sixth, they also need to establish a close relation with the commander. Seventh, coordination is also requisite between information operations and other operations. Eighth, since in military operations other than war the military works alongside other international actors, information operations must be coordinated with external actors such as the United Nations, the World Bank, and a host of non-governmental organizations. Finally, a clear end state must be articulated.

The final article in this section, Timothy L. Thomas' "Kosovo and the Current Myth of Information Superiority," explores several aspects of the role of information operations and information superiority in NATO's involvement in the conflict in Kosovo. Although Thomas argues that "conditions were right for NATO to achieve total information superiority," he maintains that NATO failed to achieve it.

But, to support this conclusion, he marshals an array of evidence. Many fewer military-meaningful targets were destroyed than at first believed. Serbian decoy efforts often succeeded. The wrong buildings were sometimes designated as targets. Battle damage assessment was inadequate. NATO communications may have been intercepted. Information was frequently delayed. Thomas' list goes on.

As a result, NATO was unable "to achieve a political or diplomatic victory." Second, NATO was unable to locate Serbia's "center of gravity, the police and paramilitaries doing the killing." Third, it did not counter rumor nor prejudiced reporting, even on an issue as critical as the number of Kosovo civilians killed by Serbian forces. Fourth, politicians affected the value of information, especially by demanding NATO planes fly above 15,000 feet to minimize casualties. Fifth, "asymmetric offsets" such as fake tanks and other decoys and Serbian analysis of NATO air operation templates allowed Serbia to "manipulate" NATO's "awareness". Finally, despite years of practice and the absence of electronic countermeasures, NATO communications occasionally experienced serious problems.

Thomas concludes by identifying and highlighting three equally unsettling problems. First, he charges that the methodologies that the United States and NATO used to evaluate data have "minor shortcomings" that "sometimes result in horrific mistakes that directly affect our credibility at higher levels." Second, he believes that the United States and NATO are "not realistically assessing the conditions under which our military capabilities are being employed." Third, he advocates that "the U.S. military must rid itself of a degree of self-deception that occasionally appears." His concern on the final point is especially poignant. "The U.S. and NATO forces are good and they know it," he accepts, but their estimates of success must improve less "manipulated figures…lead to unrealizable goals or expectations."

What, then, will war in the Information Age be like, and how will it be fought? Will the United States and its allies be able to use information superiority to dominate militarily? Or, as in Kosovo, will they be able to dominate militarily but nevertheless be unable to achieve a political or diplomatic victory? Will countries that are militarily inferior to the United States be able to exploit U.S. vulnerabilities and dependencies by using information warfare and other means of asymmetric attack? Will the United States in military operations other than war find ways to better integrate its information resources with its other political, diplomatic, and military resources so that it can better achieve its aims? Or will sub-state actors ranging from warlords in developing states to terrorists in the developed world rewrite the lexicon of the way conflicts are fought? Clearly, postulated scenarios for the future and the experiences of the 1990s provide a broad range of possibilities for which planners and strategists must prepare.

CHAPTER 17

A FAILURE OF VISION
(retrospective)

By
Fred Kennedy, Rory Welch, and Bryon Fessler

PYONGYANG, KOREA, 2013. "Defeating the United States was a much easier task than we thought possible," Col Myong Joo Kim said in precise English. Educated at Harvard and CalTech, the haggard 45-year-old North Korean stood at the head of a small table around which sat interested representatives from nine nations. The room was harshly lit, without windows, and electronically screened from the outside world by systems "borrowed" from their prostrate foe. Colonel Kim's speech would never be heard again outside this forum, and the representatives would rapidly disperse after the briefing. However, it was essential for each representative to understand the nature of the successful campaign against the Americans and the implications for his nation. Colonel Kim announced:

> *Our plan has succeeded. We have inflicted—to paraphrase the words of an American airpower theorist—a "strategic paralysis" on the United States so that it is incapable of acting.*[1] *Following our attack on their homeland, the Americans have become defensive, turning decidedly inward. Their influence is rapidly*

> *waning around the globe; no longer do they deserve the title, "superpower." The remainder of the 21st century is wide open.*

Some congratulatory glances were exchanged. Colonel Kim noticed these, then glanced down at his notepad. He spoke louder:

> *Please do not make the mistake of assuming that this outcome was a foregone conclusion. The United States remains very powerful. There were specific steps that the Americans could have taken that might have prevented us from succeeding, or stopped our efforts in the planning stage. However, to be blunt, they suffer from a rather distressing lack of vision. Their own military strategy documents of the late 1990s anticipated much of the multipolarity and rapid change that have shaped the world of the 21st century—something that we in part helped to precipitate. As the world's last superpower, they acknowledged the dangers posed by aspiring regional powers, the proliferation of advanced weapons, terrorists, and attacks on their homeland.[2] However accurate their predictions of the future might have been, they made the mistake of continuing to structure their armed forces for combat between large numbers of conventional forces[3] while paying only lip service to the threat of asymmetric attack. Their arrogance blinded them to the possibility that a potential adversary might actually try to achieve their ends by other than a direct military confrontation. Their folly allowed us to exploit vulnerabilities in their most vital high-technology systems, making the*

> *dominance of their conventional forces irrelevant.[4] We should not fault them too much. Events have proceeded apace. Without an easily understood and measurable foe, the Americans have floundered for almost 20 years. It is certainly true that they have upgraded their systems along the way, but they never were able to fully realize the true value of their most technologically advanced systems, those that operate in two closely coupled media—space and information. We were able to take maximum advantage of their plodding and uncertainty. Let me start at the beginning. Like any other nation, the United States is a complex system, and despite its many protests to the contrary, it has systemic weaknesses and leverage points that can be exploited by a knowledgeable adversary.*

The Plan

RANGOON, MYANMAR, 2009. The first meeting was shrouded in the utmost secrecy. The principals, with a suspicion verging on outright paranoia, shuttled through several unlikely ports of call before finally arriving at their destination. Initial communications were by word of mouth. There would be no “smoking gun” in the form of a document or cellular phone call to betray those involved. All participants prepared decoys who appeared prominently in foreign cities to distract the attention of the American intelligence-collection system. One joked nervously that he was less concerned with potential Central Intelligence Agency (CIA) ferrets than with the ubiquitous representatives of the U.S. media. One reporter might suspect a ruse and inadvertently stumble on a story larger than he or she could easily imagine.

The Iranian envoy spoke first. He had not only originated the initial plan but had taken the potentially risky step of personally contacting the other members—representatives from North Korea, China, Iraq, and several multinational corporate concerns. He spoke of the "artificial restraints" currently imposed upon the world by American might, the inability of nation-states to exercise their freedom, and the absolute preeminence of the United States in the technical, industrial, and military realms. "Rome was no greater a power in its day," he remarked, "and Rome endured for centuries. The Pax Americana is less than a century old. How long must we endure it?"

Nods and shrugs. The discussion quickly turned to the magnitude of the problem facing the cabal. The Iraqi envoy noted that his country had attempted to stand its ground with the best weapons it could afford only a generation previously but that it had been thoroughly trounced by the American war machine. The Iranian countered that the Iraqi challenge had been foolhardy, based as it was on meeting American strength directly. "Let us not tempt their stealth fighters and their carrier battle groups. We cannot best them. We are not—with the possible exception of my able Chinese friend—'peer competitors.'"[5]

"What, then?" asked the North Korean. "Terrorist attacks? Car bombs and suicide squads? What you seem to be suggesting is a route that has been attempted but that is felt to be no more than a pinprick by such a giant." The Iranian smiled and gave his reply:

> *Like any other nation, the United States is a complex system, and despite its many protests to the contrary, it has systemic weaknesses and leverage points that can be exploited by a knowledgeable adversary. First, we will attack its leadership directly and audaciously. We will then undertake to seriously damage its command, control, and communications infrastructure. Finally, we will assault the economic infrastructure of several major cities.*
>
> *Some of you are clearly asking, "To what end?" The answer is simply put: to make them withdraw, to turn inward. The Americans are insular by nature, and they are still not entirely comfortable with the leadership role history has thrust upon them. Our attack will exceed their "cost-tolerance"[6] for continued conflict, at which point they will retreat to North America and wall themselves in. Such a course of events will permit us a free hand to take what is rightfully ours, unhindered by American intervention.*

There were nervous shuffles and uncomfortable looks around the table. The Chinese representative spoke up. "We must not provide the United States with a valid target. They will want to lash out, and may perhaps do so irrationally. Therefore, all strikes must be covert strikes. We shall undertake no high-profile efforts that could warrant direct retribution against a specific nation."

"That is precisely what I have in mind."

Stage 1 (Decapitation)

11 July 2012, 8:35 a.m. EST. The day dawned hot, humid, and calm, typical of this time of year in the Washington area. Commuters inching north along I-395 glanced up through sunroofs to notice a low-flying twin-engined plane following the freeway at an altitude of only 100 feet. Of these, only four had the presence of mind to call in complaints on their cellular phones, but these calls were ignored by dispatchers as likely cranks. The aging 1972 Beechcraft King Air E-90 had already been airborne for over 3 hours, angling northeast across farmland and forested hills after an uneventful predawn takeoff from a private field east of Roanoke, Virginia. This course had been selected after only the most careful consideration of the alternatives—including a launch from one of the numerous supertankers plying their way up and down the East Coast. The conspirators had decided that the U.S. air defense network of phased-array radars, Air National Guard and Customs patrols, aerostats, and the occasional overflight by low-orbit satellites carrying synthetic aperture radars (all enlisted in the continuing war on drug trafficking) was sufficiently daunting to make an unnoticed approach to the coast a chancy proposition. However, one member of the team pointed out that the North American Aerospace Defense Command (NORAD) was not nearly as interested in happenings within the interior of the country. Furthermore, U.S. air traffic controllers often viewed only their transponder data, not bothering with the cluttered and headache-inducing radar return. A light plane running low and with its transponder off could thus be virtually invisible. Acquiring the plane and smuggling in the “munition” became the largest

stumbling blocks, but the North Korean "team" overcame these obstacles with relative ease.[7] All had dispersed within minutes of the plane's takeoff and were headed for international flights from several different airports in the Southeast.

Guided by a vastly improved global positioning system (GPS) network[8] and assisted by sophisticated terrain-mapping software[9] (downloaded from a French Web site), the King Air carried no living human cargo—although a freshly thawed corpse was strapped into the pilot seat. The airplane dipped to under 50 feet as it passed between the Pentagon and Washington National Airport, cruising within the ground clutter, and then it abruptly began climbing, dispensing innumerable spores of multiply resistant Bacillus anthracis across much of the central capital area.

Suddenly alerted to the small plane's presence, air traffic controllers at the airport and at Andrews AFB, Maryland, tried at first to contact the aircraft and then began to narrowcast warnings to the Secret Service and other agencies. After several minutes, however, the aircraft veered to the northwest, dove rapidly, and crashed into the bluffs above the Maryland side of the Potomac, across from CIA Headquarters. The resulting fireball was extremely hot, leaving eager investigators and media little evidence other than melted wreckage and charred bone fragments. One observer reported weeks later that she had seen the small aircraft drop a cylindrical object as it flew over the Potomac, just prior to impact.

"Inhalation anthrax"[10] announces itself with initial symptoms easily mistaken for the flu or a common cold. Within 2 days, approximately 250,000 people—

including the president, the vice president and her husband, 160 senators and representatives, senior leaders from numerous federal agencies, three service chiefs, and more than 11,000 Pentagon employees began to experience low-grade fever, fatigue, and a slight cough. Of the few that bothered to notify their doctors in the critical hours following the attack, none received the correct—and fatal—diagnosis. Ninety percent of those infected would die within a single week. The ensuing chaos would plunge the entire country into confusion.

Colonel Kim continued:

> *We killed a significant portion of their national leadership with a single blow—the president, vice president, and several cabinet members, along with a host of their military leadership. Yet we left no traces for them to follow, and there was little opportunity for a coordinated investigation in any event, given our next actions. Now, the Americans could have prevented this if, for instance, they had carried out their plans for a space-based radar or global air traffic control system. Their current surveillance is spotty at best—and despite their professed concern about terrorism, they are egregiously poor at deterring internal threats. Even a fairly rudimentary low- or medium-orbit constellation of radar satellites providing continuous wide-area coverage could have detected our aircraft in time to take action.*

The Iranian envoy frowned and said, “We had initially thought that their space systems were among their strongest assets.” Kim replied,

> *Yes, and you were correct to think so. However, we quickly discovered significant gaps in their existing reconnaissance and surveillance architecture. Certainly, they were—and are—able to detect virtually anything that moves on or above the earth, but in very circumscribed regions, and for only short periods of time. Without a global network, they must deduce which areas are of interest for observation, and either wait for their satellites to pass over the target or command them to modify their orbits. The first is time-consuming, while the second wastes precious fuel.*
>
> *U.S. leaders never succeeded in developing either the doctrine or the systems required for space denial and space protection. In fact, their national policy proscribed such activities, despite the obvious vulnerabilities of their vital space assets.*
>
> *In short, the United States failed to capitalize on its initial investment—and continued to rely on an immature intelligence architecture. It hid behind its superior technology but failed to close the gaping holes in its systems.*

Stage 2 (Disruption)

15 July 2012, 11:40 a.m. EST. Thousands of cases of severe respiratory distress were being reported all across the national capital region—alarming doctors and patients alike. Some 2,000 people had already succumbed to “an unknown viral or bacterial infection.” Widespread panic engulfed the District of Columbia metro area following the Center for Disease Control’s (CDC)

announcement of a regional quarantine on travel. With very little yet to go on, investigators from the CDC and the Army's Institute for Infectious Diseases were out in force, searching for answers. A regional manhunt was on, with few obvious suspects. Even as it was becoming clear that the national capital had been subjected to a catastrophic biological attack, it was evident that there was very little that could be done for the victims. The president was said to be gravely ill and several of his advisors incapacitated. Major news outlets were scrambling for information. Cable News Network (CNN) placed the story at the top of the lineup for its midday news summary, despite the skimpy nature of the material. Most other networks followed their lead. These reports were destined to never make it on the air.

Some 35,000 kilometers overhead, a nondescript Chinese telecommunications satellite, Dong Fang Hong (DFH) 91, sat idle in a "supersynchronous" orbit.[11] The Chinese had launched the satellite over a year and a half earlier, but it had suffered a series of highly publicized technical problems and was grudgingly relegated to the "junk belt" beyond geosynchronous earth orbit (GEO) in January 2012. Perhaps as a final insult to its builders, DFH 91 failed completely after performing its apogee boost and now revolved in a "useless" 26-hour orbit, returning to geosynchronous altitude at a slightly different longitude every day.

In reality, DFH 91's status as a derelict applied only to its ability to transmit digital TV to Chinese viewers on the planet below. Beginning in April, an observer positioned near the satellite would have noticed something out of the ordinary. Upon each descent of DFH 91 to the geosynchronous belt, a small dark object not much larger than a football would be ejected from a rear panel of the satellite. As it floated away from its parent, the small object would flare brightly and begin to recede, braking its way into a true geosynchronous orbit.[12] DFH 91's patient ground controllers would time these events to occur only over the daylit side of the planet; after all, even an enterprising amateur astronomer might have spotted the brief but brilliant pulse during an evening's comet hunting.

By late June, nearly 90 of these odd vehicles had been deposited around the GEO ring like so many spaceborne mines. All had benefited from the GPS's recent addition of "aft horns," allowing satellites in GEO to take advantage of America's premier navigation system to find their way. All had performed co-orbital approaches and were scant meters from their targets, awaiting the final order to rendezvous. The targets, 86 diverse satellites built and launched by a half dozen nations, sat blissfully unaware, most receiving and transmitting video and voice data to waiting customers on the planet below. Other "birds" gathered weather data or listened to the encoded electronic whispers of a billion conversations. Some waited patiently to report the telltale bloom of a ballistic missile launch or nuclear detonation.

The targeting itself was indiscriminate—and purposefully so. The Chinese knew that they would lose three satellites of their own in the attack. This was deemed an acceptable loss, and a useful misdirection. After all, there were still fewer than 20 states that could have managed the launch of a geostationary satellite, and suspicion would quickly settle on just one or two.

The final order was in fact no order at all. In the event of an abort, DFH 91 would have suddenly and surprisingly come to life, broadcasting a strong encrypted message to its kill vehicles strewn throughout the GEO ring. The vehicles would have immediately shut down, and the Chinese would explain the anomalous event as one more example of the satellite's bizarre behavior.

No abort was issued; the kill vehicles obligingly proceeded to "dock" with their targets. Most satellites are "hardened" against the severe radiation environment of space; some are further hardened to withstand the radiation concomitant with a nuclear blast. Few are armored against physical assault, other than to mitigate the effects of continuous micrometeoroid bombardment. After all, armor is heavy, and weight is at a significant premium when the cost of lifting a single kilo to orbit exceeds $50,000.[13] Thus, it was quite unnecessary to construct sophisticated kill vehicles. The simple devices simply exploded in close proximity to their satellites, sending shrapnel through solar arrays, battery systems, onboard computers, guidance systems, and sensors alike.

Sixty-two satellites were completely destroyed. Ten more were severely damaged and able to provide only marginal capability. Fourteen were apparently undamaged—most likely due to a faulty trigger on the kill vehicle or badly executed terminal maneuvers. The roster of casualties included Intelsat 919 (broadcasting 20 channels of video to various Arab nations), Thaisat 7 (providing mobile communications to Southeast Asia), and Gorizont 80 (a Russian military communications satellite).

None of these losses were made immediately apparent to Americans. However, at 9:43 a.m., Mountain

Standard Time, controllers at the Space Based Infrared Systems (SBIRS) II[14] ground station at Falcon AFB, Colorado, were startled by the simultaneous loss of signal from fully three of their GEO birds. These satellites surveilled the planet for the infrared signature of ballistic missile launches. Without them, the United States would have to rely entirely on its groundside radar sites for detection of incoming missiles. A mad search for answers began to leap up the chain of command. A similar panic was setting in at the control center for Milstar III[15] communications satellites, where half of their birds had suddenly gone dark. Automatic rerouting systems looked for the next satellite in line to relay the growing backlog of message traffic, and, finding none, began sending queries and alarms to the control centers. Secure communications were crashing across the planet. In the anarchy that followed, the secretary of defense was forced to use land lines, ordering U.S. military forces around the globe to their highest state of alert. No opponent had yet bothered to raise its head.

As the military scrambled to respond to an unknown threat, civilian controllers watched in horror as CNN's five network broadcasts went down simultaneously. Iran's Voice of the Islamic Republic, broadcast on nine channels, vanished into static. Viewers in Southern California lost all 460 channels of GlobalNet LA. Local television affiliates, adrift without their normal satellite feeds, began placing calls to network broadcast centers, looking for answers that were simply unavailable. In a matter of minutes, the United States had lost 43 of its satellites in GEO, devastating military and civilian constellations alike. Fully two-thirds of the data shuttling between GEO and earth suddenly had nowhere to go.

What the United States needed was a few simple systems and the doctrine to tie them together.

Despite this, none of the personal communication and mobile telephone systems, provided by satellites orbiting at much lower altitudes, were destroyed. Between 11:30 a.m. and 1:30 p.m., call volume over these systems tripled, then quadrupled. By early evening, it was virtually impossible to secure a phone line anywhere in the country. The ubiquitous World Wide Web, repeatedly overhauled and massively enhanced during the first decade of the 21st century, was suddenly jammed with billions of demands for news. The information flow first slowed, then stopped. There was little enough to be had in any event.

Colonel Kim pointed to the statistics flowing down the wallscreen behind him:

> *In all of this, we never engaged a single American weapon system. U.S. leaders never succeeded in developing either the doctrine or the systems required for space denial and space protection. In fact, their national policy proscribed such activities, despite the obvious vulnerabilities of their vital space assets. The unspoken consensus among their commanders was clearly that space itself was too vast and the technologies needed were sufficiently difficult to develop that few other nations could devote the necessary resources to acquiring them.*[16] *Further, it is now clear that the United States was confident that it could spot a "rogue" launch and antisatellite attempt, trace it to the*

> *offending nation, and mete out punishment through more conventional means—via air strikes, for instance. The highly clandestine nature of the Chinese attack thwarted this, and left the United States without an adversary on which to concentrate.*

"Yet we must certainly be high on their list of suspects," the Chinese representative pointed out. Kim nodded and said:

> *Yes, and for this very reason we insisted on a plan which would foil even a determined investigation. Even so, discovery after the fact was not our greatest fear. In the midst of the confusion we created, with the chain of command disrupted, it was entirely possible that the United States might jump to conclusions and lash out blindly.*

Colonel Kim shook his head in mock concern, then continued:

> *The biological attack might have been seen as domestic terrorism, but an attack on space assets could be attributed to none other than a foreign power. Yet, even today, U.S. leaders remain uncertain. Their ground-based assets were able to tell them that their satellites had been physically damaged or destroyed, but the lack of space-based reconnaissance systems has severely hampered their attempts to identify their foe.*
>
> *What the United States needed was a few simple systems and the doctrine to tie them together: a highly mobile reconnaissance platform to perform*

> *on-demand, close-in imagery; perhaps a variant of the same platform to damage a hostile satellite or tow it to a nonthreatening orbit; some form of proximity detection and defense for their most prized assets, such as their early warning satellites; and a rapid, ultra-low-cost launch capability to replenish constellations during a crisis. Finally, and most importantly, there was the need for an overarching concept of operations to integrate these basic missions. Without these elements, the U.S. space architecture was immature, completely wedded to remote sensing and communication—in essence, subservient to their information architecture. Unable to conduct either offensive or defensive space operations, the existing American space order of battle—if we can so dignify it—calls to mind nothing so much as their Civil War–era ballooning efforts, the first crude attempts at overhead reconnaissance: virtually un-maneuverable, vulnerable to fire from below but unable to return fire. And yet, the United States was eventually able to achieve a fearsome mastery of air warfare, despite a somewhat unpromising beginning. In space, however, it remained stubbornly unwilling to make the logical leap.*

The Iraqi piped up irritably, “For what purpose do you tell us where the Americans failed?” Kim pointed a finger at the Iraqi and said:

> *I tell you this because our coalition must now begin to consider these very issues if we wish to someday gain hegemony. We have learned much from the U.S. defeat, and if we do not take advantage of this momentary lapse in*

> *American attention, our efforts will have been for naught. In a very real way, we have surpassed them.*
>
> *They believed themselves to be, technologically, several generations ahead of their competition, which made them complacent. They chose to forget that a true revolution in military affairs—I use their terminology—requires not just the systems but a sophisticated operational doctrine to support them.*

Stage 3 (Pandemonium)

15 July 2012, 1:54 p.m. EST. The CDC issued a sporadically heard statement at this hour, declaring the capital a victim of a biological attack. Emergency Broadcast System messages began playing at local Washington, D.C., affiliates just before 2:00 p.m., asking the populace to remain calm and stay in their homes. This warning went unheeded. Highways around the region were closed to inbound traffic entirely, freeing up additional lanes to the fleeing public. National guardsmen from Virginia and Maryland, requested by the president early in the afternoon as riots began to erupt around the District, found themselves stranded along the shoulders of major arteries, waiting out the passage of hundreds of thousands of panicked residents in the D.C. area.

As panic gripped the national capital region and the military groped for answers, the final phase of the coalition attack began. It had already been initiated by a scrambled cellular call, placed from Teheran to Norway at just after 9:50 p.m. Iranian time. In a quiet Oslo suburb, a "go" was given. Led by the notorious hacker “Whisper,” three seasoned programmers set to work, bouncing the ignition signal of a particularly potent virus off three telephone switching stations in Britain, and finally through commercial Web sites on both the East and West Coasts of the United States. The effect was immediate: automated teller networks in six major cities—Los Angeles, San Francisco, Seattle, New York City, Miami, and Washington—were instantly brought down. Those that returned to service began to behave erratically, releasing thousands of dollars at the touch of a button. Los Angeles–based banks responded almost instantly, closing their doors on mobs of angry account holders in the early afternoon. Lending institutions across the country began to follow California’s lead, creating a growing ripple of uneasiness. The run on hard currency was beginning. The New York Stock Exchange suspended trading half an hour before the closing bell; the market had already slipped an ominous 15 percent. Despite the frustrating communications backlog, realization was spreading that the United States appeared to be under some form of diverse, coordinated assault. In Oslo, Whisper prepared to unleash a second attack.[17]

They [the Americans] chose to forget that a true revolution in military affairs…requires not just the systems but a sophisticated operational doctrine to support them.

The target was the already overloaded U.S. telephone network and its collection of switching and routing stations.[18] Cellular grids and telephone exchanges in the D.C. area received special attention, although outages were initiated in seemingly random locales from Colorado Springs to Charleston. The net effect of the attack was to bring nationwide commercial telecommunications to a standstill. Coupled to the crippling blow dealt the banking industry, economic transactions ground to a halt. In contrast, vital national communications were left untouched. The military's workhorse Defense Switching Network (DSN), the Joint Chiefs of Staff Alert Network (JCSAN), and the Secure Voice Teleconferencing System (SVTS) remained fully operable.[19] Information warfare experts were awakening to the fact that they had been as effectively bypassed as the Maginot Line in 1940.[20] What none had yet understood was the magnitude of the disaster. Whisper's viruses would confound some of the best American programmers for months. The heavily encrypted Iranian software had been designed to resist the most concerted decoding attempts.

Word of the president's death by severe respiratory distress arrived shortly after the dinner hour on the East Coast, and reached the rest of the nation and the world primarily through shortwave radio transmissions. With the vice president already dead, the Speaker of the House, a senior Democrat from Pennsylvania, was transferred by helicopter to Andrews AFB. At 6:55 p.m., the Speaker boarded the nation's single E-5D, a highly modified Boeing 777, and the latest in a long line of aircraft that had waited to perform this mission. As the plane became airborne, one of the three surviving Supreme Court justices administered the oath of office to the badly shaken congressman, whose first act was the declaration of martial law nationwide. His second act, perhaps more controversial, transferred the official seat of government from Washington to Philadelphia "for the duration of the crisis."

Americans in all walks of life awaited their opponent's next move. Colonel Kim pointed to the Iraqi envoy:

> *In 1990, the United States perceived your incursion into Kuwait as a serious threat to its national security. Why? Your nation hadn't fired on any Americans. Your crime was to endanger their oil supplies. They responded with prompt action, and you and your countrymen were humiliated.*
>
> *The Americans saw the threat to their information networks even as they were constructing them. Their military built elaborate security measures to resist intrusions into secure areas, protecting sensitive data and preventing unwelcome visitors from wresting control. Yet even as they strengthened these defenses, they did not pay sufficient attention to the massive growth of their nation's commercial information infrastructure, and their economic reliance upon it. The analogy between oil and information could not be clearer—banking networks and telecommunications systems are, if anything, more essential to the day-to-day operation of their country, and far more vulnerable to disruption.*
>
> *Our Iranian allies chose well, attacking vulnerable civilian systems and ignoring the heavily protected government networks. By itself, such an effort would have resulted in irritation and annoyance. Coming on the heels of the other attacks, however, our information strike resulted in a mass hysteria which, for all practical purposes, temporarily shut down the United States. While they were able to reconstitute their government fairly quickly, they have still failed to fully recover.*

> *Their citizenry is up in arms and demanding answers. For the past year, their legislators have been calling for a "retrenchment."*

"I trust that you all understand why I am spending some time on how the Americans might have defeated us?" Kim asked. There were nods of assent around the table.

> *One lesson we have learned is that information warfare is not to be applied in a vacuum.*[21] *In concert with other forms of war, it can have useful synergistic effects. Taking out a city's electrical power is an inconvenience, but it is not typically life-threatening. But to the same city gripped in the throes of rioting, such a move can be devastating.*
>
> *Countering our information strikes would have required a coordinated effort on the part of the American military establishment to protect "critical sectors"*[22] *of the commercial information infrastructure. This would have been a daunting task. American corporations are noted for their fierce independence; they would have chafed under any form of regulatory guidance the government imposed. Yet forgoing any form of protection foolishness—after all, one should not depend on that which one cannot defend.*

Colonel Kim switched off the wallscreen. In a grave tone, he continued:

> *The United States was able to marshal its enormous scientific and engineering expertise to create invention after invention for space and information applications. Americans built high-technology houses of cards and congratulated*

> *themselves on their innovation without taking the time to fully understand the full implications of what they had wrought. They dabbled in remote sensing, providing themselves an illusory sense of security at odds with their actual capabilities, and leaving themselves open to unconventional attack. They refused to apply their own lessons of airpower to space power, preferring to maintain a fragile and highly vulnerable information architecture in the sky. Lastly, they chose not to tackle the admittedly difficult problem of safeguarding their civilian information infrastructure. Taken in isolation, each of our attacks was painful but not threatening to their national integrity. Together, however, they very nearly brought the United States to its knees.*

The North Korean envoy rose and bowed expansively, "Thank you, Colonel Kim. Your analysis is a cogent one, and I assure you it is greatly appreciated by each of us. I apologize for not remaining; I go now to oversee the last of the mopping-up operations around Pusan. Please, know my gratitude and that of your nation."

Epilogue

History will record that the United States suffered a resounding defeat in 2012 by an anonymous adversary employing a combination of low- and high-technology thrusts that skillfully brought the world's last superpower to its knees. Emboldened by the emergence of this power vacuum, numerous nation-states rushed to pursue territorial expansions that would have been unthinkable in another era. North

Korea, hanging on long after pundits had predicted its fall from famine, brutally seized the South with chemical and biological weapons in 2013; 3 years later, China moved southward into the newly emergent industrial powers—Laos, Cambodia, and Vietnam—of the Asian Dynamo. After initially threatening a nuclear response, an exhausted Israel capitulated to a combined Islamic force in 2029.

In all of these crises, the worldwide question was the same: Where were the Western powers? Without strong U.S. backing, Europe was essentially impotent, unable or unwilling to come to consensus decisions. Russia, continually wracked by internal civil strife, could not shift its focus away from preserving the remains of its shattered empire. While the United States was able to recover and rebuild itself following the initial shock, it was simply incapable of responding to foreign crises. Fortress America had been breached, and the citizenry was adamant that it would never happen again. The rest of the world would, for the most part, be left to its own devices.

[1] John A. Warden, "Air Power for the 21st Century," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell AFB, Ala.: Air University Press, 1995).

[2] These potential threats to U.S. interests are discussed in the *Report of the Quadrennial Defense Review* (QDR) (Washington, DC: Department of Defense, 1997), 3–4. The full text is on-line at http://www.defenselink.mil/pubs/qdr/

[3] *Ibid.*

[4] The *Report of the QDR* did acknowledge that future adversaries may use terrorism; nuclear, chemical, and biological (NBC) threats; information warfare, or environmental sabotage to attack our forces or interests overseas and at home. However, such threats were viewed only in the context of how they might adversely impact our conventional military operations (p. 4).

[5] The *Report of the QDR* notes, "The security environment between now and 2015 will also likely be marked by the absence of a "global peer competitor" able to challenge the United States militarily around the world as the Soviet Union did during the cold war. Furthermore, it is likely that no regional power or coalition will amass sufficient conventional military strength in the next 10 to 15 years to defeat our armed forces, once the full military potential of the United States is mobilized and deployed to the region of conflict" (p. 5).

[6] Cost-tolerance is defined as the point at which the cost of accepting an adversary's policies, in terms of deprivation and suffering, is less than the cost of continued resistance. Dennis M. Drew and Donald M. Snow, *The Eagle's Talons: The American Experience at War* (Maxwell AFB, Ala.: Air University Press, 1988), 6–7.

[7] Airplanes On-Line advertises numerous light planes for sale (http://www.airplane.com/). One of the authors was easily able to locate several aircraft with the necessary range, one right over the Virginia border in North Carolina, and the asking price was not exorbitant.

[8] The U.S. Naval Observatory's web site (http://tycho.usno.navy.mil/gpsinfo.html/) speaks to current GPS capabilities. The Standard Positioning Service (SPS) permits a vertical fix accurate to approximately 156 meters (511 feet), insufficient to fly "nap-of-the-earth." GPS's Precise Positioning Service (PPS) provides substantially improved performance, allowing for a fix of 28 meters (92 feet) or better. Originally, PPS was to be made available to nonmilitary users on a case-by-case basis; however, a 1996 presidential directive specifically called for the more accurate signal to be made available to civilian users by 2006. Differential GPS—using ground reference receivers—makes "sub-meter" determination possible, without any of the additional enhancements currently planned by the NAVSTAR GPS Joint Program Office for its Block IIF satellites. Some discussion of this can be found at http://www.arpa.mil/ARPATech-96/slides/ganz/100

[9] Digital terrain modeling software is easily available today via the Internet through numerous commercial outlets. The authors were able to download demonstration versions of both American and New Zealand models. It is not unlikely that 12 years from today highly accurate terrain maps, updated via imaging satellites (such as France's SPOT) will be available for perusal almost in real-time. This practice is not limited to commercial concerns; the U.S. Geological Survey maintains a web site (http://www-nmd.usgs.com) where precise topological maps of the nation's countryside can be purchased.

[10] Part II (Biological) of the Handbook on the Medical Aspects of NBC (Nuclear/Biological/ Chemical) Defensive Operations describes the effects of inhalation anthrax as well as the woeful state of potential countermeasures. It can be found on the World Wide Web at http://www.nbc-med.org/amedp6/PART II. A more detailed discussion is available in Dr. Malcolm Dando's *Biological Warfare in the 21st Century* (London: Brassey's [UK], 1994). On page 34, Dando notes, "Infection through the lungs is particularly dangerous…[inhalation anthrax] has a mortality rate approaching 100 percent."

[11] Dong Fang Hong 91 is depicted as the latest of an existing series of Chinese satellites. For instance, DFH 41, a telecommunications satellite launched 29 November 1994, was retired only a few months later, ostensibly due to a fuel leak. Numerous satellites sit in the "junk belt" beyond GEO, moved out of their precious slots to make room for other, newer assets. These moribund devices are said to have been "supersynched." For an excellent description of current satellites on orbit, point your web browser at http://www.telesatellit.com/tse/online/, the on-line edition of the Satellite Encyclopedia.

[12] Boeing's Kinetic Energy Anti-Satellite Technology (KE-ASAT) program is a potential prototype of the Chinese "kill vehicles" aboard DFH 91. See "KE-ASAT Prototype Tracks Target in Edwards Hover Test," *Aerospace Daily*, 13 August 1997, 239.

[13] The Developmental Planning Directorate at Air Force Materiel Command's (AFMC) Space and Missile Systems Center (SMC/ XR) estimates the current cost of a Titan IV launch to approximate $500 million. Since Titan IV, coupled with a Centaur upper stage, can deliver 5,200 kg to geosynchronous orbit, the cost per kilogram to GEO is slightly more than $95,000 per kilo.

[14] SBIRS (Space-Based InfraRed Systems) is the follow-on to the Defense Support Program (DSP) series of satellites, and is intended to provide missile warning, missile defense, and "battlefield characterization" information to earthside users. SBIRS is currently considering a bifurcated architecture of "high" (GEO- and Molniya-based) and "low" (low earth orbit-based) vehicles. The first SBIRS high satellite is likely to come on-line in early 2002. Mission and schedule information were found on the SBIRS web site http://www.laafb.afmil/SMC/MT/sbirs.htm

[15] Milstar III is a fictional extrapolation of the existing series of secure military communications satellites. More information can be found at http://www.laafb.af.mil/SMC/MC/Milstar/

[16] These commanders were also supported by the pacifistic nature of extant space law: “States Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.” Taken from Article IV of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies, signed 27 January 1967. Liberally interpreted, this passage has been used to attack the emplacement of any form of weapon in space. The full text of the “Outer Space Treaty” is on-line at http://www.spfo.unibo.it/spolfo/SPACELAW.htm

[17] Spectre-Press’s web site (http://www.spectre-press.com/) offers its customers a “monumental” instruction book on a vast array of dubious activities, including guidance on sending fake electronic mail messages, “cracking” Novell Netware, and getting into all manner of systems (from credit bureaus and banks to government networks). Numerous other hacker sites exist, catering to a growing subculture of covert cyber-criminals.

[18] Richard Szafranski, “A Theory of Information Warfare: Preparing for 2020,” *Airpower Journal* 9, no. 1 (Spring 1995).

Colonel Szafranski notes on pages 61–62, “In the case of advanced societies or groups, attacks against telecommunications systems can wreak havoc with an adversary’s ability to make effective decisions in warfare.” This article can be found at the College of Aerospace Doctrine, Research, and Education (CADRE) site (http://www.airpower.maxwell.af.mil/airchronicles/apj/szfran.html)

[19] The Defense Information Systems Agency (DISA) maintains a list for these and other frequently used acronyms at http://www.disa.mil/org/acronym.html. JCSAN permits the joint chiefs access to secure, on-call voice communications with all specified and unified commands. SVTS is described as an executive-level network (president/White House to secretaries) that includes packetized data networking, broadcasting, and video teleconferencing capabilities. Systems such as these are likely candidates for enhancement and expansion over the next decade.

[20] Martin C. Libicki echoes this concern in the introduction to his excellent *Defending Cyberspace, and other Metaphors* (Washington, DC: National Defense University Press, 1997). He states, “Global computer and media networking carries risks, even if these risks are easily exaggerated. Computer networks might permit enemies to use hackers to attack the information infrastructure of the United States, rather than its military forces. The conventional defense establishment has been described as a Maginot Line, in which hackers are equivalent to Guderian’s Panzer Korps, wheeling past prepared defenses to strike at the nation’s unguarded flanks.” The full text is available at the Institute for National Strategic Studies’ home page on NDU’s web site, http://www.ndu.edu/

[21] *Ibid*. The author rightly wonders, “How much damage could a digital Pearl Harbor cause? Suppose hackers shut down all phone service (and, say, all credit card purchases) nationwide. That would certainly prove disruptive and costly, but as long as recovery times are measured in hours or even days, such an attack would be less costly than such natural events as a hurricane, snowstorm, flood, or earthquake—events that have yet to bring the country to its knees.”

[22] *Ibid*. Key sectors should include telecommunications, energy, funds distribution, and safety systems.

CHAPTER 18

THE IW THREAT FROM SUB-STATE GROUPS:

AN INTERDISCIPLINARY APPROACH

By
Andrew Rathmell, Richard Overill,
Lorenzo Valeri, and John Gearson

Introduction

This paper is concerned with answering the question: What is the extent and nature of the Information Warfare (IW) threat from sub-state radical political groups? Although there has been a great deal of speculation and theorising about the potential threat from terrorist groups, there has been little open source research on this subject. Even at a classified level, it appears that intelligence agencies are struggling with the construction of methodologies for threat assessment.

This paper provides a preliminary discussion of findings from a research project underway at ICSA. The concept behind the project is the assumption that assessing the IW threat from sub-state radical groups requires the combined skills of computer and information security specialists, strategists, and political scientists with area expertise.

The information revolution presents today's terrorist organizations with new opportunities to pursue their political and strategic aims. The Internet in particular can be used to spread their message by making it accessible to audiences world-wide. At the same time, weaknesses in networked systems can be exploited to raise funds or to attack Government Information Infrastructures (GII) and National Information Infrastructures (NII). As noted by Walter Laqueur "…why assassinate a politician or indiscriminately kill people when an attack on the electronic switching will produce far more dramatic and lasting results?"[2]

Scope and Definitions

For the purposes of this study, the following definitional limitations have been adopted:

1. the only forms of IW that are considered are software warfare and psychological operations;[2] and

2. the concentration is on assaults on civilian and strategic targets.

Direct attacks on the Defence Information Infrastructure (DII) are not considered. Attacks on the NII however pose a threat to the military due to its growing reliance on the NII for operations and administration.

Structure and Content

This paper has three parts:

1. a discussion of the techniques of software warfare;
2. a theoretical discussion of how terrorists may use IW. This section will also consider the sociological traits of hackers and outline their environment; and
3. an empirical analysis of selected terrorist groups.

This section will look at the strategies, the organizational culture and the self image of terrorist organizations.

Software Warfare

Terrorist activities in cyberspace may be considered as part of a new kind of war: software warfare.[3] When InfoWarriors plan to hack or penetrate particular networks, their goal is to modify software and, consequently, its proper functions. Conversely, the system managers of the targeted information systems have to make sure that software is protected and running properly. Other forms of Information Warfare, such as Command and Control Warfare (C2W), Information Infrastructure Warfare (I2W) or economic information warfare are therefore dependent on the outcome of this competition to control the software of information systems.[4]

Software Warfare Techniques

Knowledge of techniques of software warfare comes from the activities of private sector hackers and crackers as well as from government-sponsored IW programmes. Software warfare generally involves two steps—penetration of a system and disruption.[5] In practice, the majority of computer/data crime or software attacks are perpetrated by a trusted user already inside the system. This is clearly one strategy with which terrorist groups are already familiar. Otherwise, they will need to penetrate the system.

In the UK, the most common penetrative strategy involves acquisition of an authorised user's password. This may be achieved in a number of ways. Packet sniffers installed on gateways, routers, or bridges linking packet switched networks can be employed to detect usernames and unencrypted passwords in transit to remote hosts; password grabbers installed as TSR (terminate and stay resident) programmes on remote workstations mimic the logon sequence of a central server in order to dupe the user into giving up their username and password. Password crackers, such as that within Crack 5.0, are employed in repeated attempts to break an encrypted password using a dictionary. Added to this, well-informed password guessing and persuasive "social engineering" are often exploited.

More general tools, such as SATAN (Security Analysis Tool for Auditing Networks), which are publicly available, are also routinely used to probe the configurational security of target Internet hosts against more sophisticated intrusion strategies.

After penetration, an intruder requiring system manager, superuser, or root capabilities will attempt to obtain these by some form of subversion, typically a Trojan Horse. Such programmes are planted to replace but mimic the actions of common system utilities, but with undocumented side-effects to benefit the intruder. Thus a system manager could unwittingly confer system-wide privileges on the intruder while executing the Trojan utility. Trojans may also have palpably destructive side-effects, such as deleting or scrambling mission critical files, and as such have been used for sabotage, extortion and blackmail.

Software bombs have a similar role to destructive Trojans. Planted (and usually well concealed) within some mission critical software, they consist of a trigger and a payload. If the trigger is a date and/or time then it is termed a time bomb. If the trigger is some logical condition it is called a logic bomb. When the host application is executed, the trigger condition is tested. If it is true then the payload is activated, often with destructive consequences. Typical sabotage scenarios involve an employee setting a trigger condition that their name no longer appears on the firm's payroll and a payload which is to delete the stock control or customer files. For blackmail or extortion, the trigger might be that the employee's salary has not been increased substantially. In either case the logic bomb would be buried in the payroll programme by the employee.

Computer viruses resemble software bombs in generally having a trigger and a payload, but differ in that they replicate themselves by attaching themselves parasitically to files or disk sectors which are going to be executed in the normal course of events. Six generations of virus are now generally recognised: benign, self-encrypting, stealth, armoured, polymorphic and macro. By the end of 1996 about 8,000 virus strains were known, but only about a dozen were "in the wild." The number of strains observed appears to almost double each year. As with software bombs, the trigger can be a date (e.g., Michaelangelo's birthday, Friday the 13th) or a condition (e.g., 99th power-up since infection).

The payload can vary from the irritating (e.g., playing Yankee Doodle Dandy or displaying bouncing ping-pong balls) to the devastating (e.g., formatting the hard disc). Different infection strategies and lifecycles have also been noted, including "slow" viruses which only infect files that are being modified by the user, "fast" infectors which infect every file opened by the user, and heteroclyte (or "tunnelling") viruses which have a three-state lifecycle moving e.g., from executable file to disk boot sector to memory and back to executable file again. In addition, virus authoring packages have also been made public. It is claimed that the Mutation Engine can produce four million, million variants of a given virus.

Virus attacks tend to be indiscriminate and difficult to target accurately since their spread depends on human carelessness or lack of vigilance as well as on their own intrinsic virulence. For this reason they are not particularly suitable for blackmail or extortion purposes. However they can cause enough general panic and mayhem to be considered as candidates for disruption to business and society at large.

Worm programmes are replicators which do not necessarily damage data. They simply consume system and network resources (processor cycles, memory capacity and communications bandwidth) by exponential growth in numbers. In so doing, they render the system incapable of performing useful work. This electronic gridlock is one form of "denial of service" attack which, when launched on an institution such as a major clearing bank, for which online transaction processing (OLTP) is business critical, can cause major financial damage and hence has great potential for sabotage, extortion or blackmail.

Terrorists and IW

How might terrorist groups use IW? This study postulates three key uses. First, to carry out propaganda campaigns. Second, to raise funds. Third, to attack the NII. The only demonstrated use so far has been in the first category but it is striking how successful small radical groups have been in leveraging Information Technologies for their psychological operations even with limited resources. The potential for using IW techniques as a force multiplier in the latter two categories is great. This section discusses the ways in which terrorists may gain access to the knowledge required for IW, specifically by tapping into the skills of hackers.

Amateur Hackers and Terrorists

Hollywood films like the 1983 “War Games” or the 1995 “The Net,” science fiction novels by William Gibson, or the complex police operations required for catching “Internet stars” such as Kevin Mitnick have exposed the world of amateur hackers to the public. Because of this world-wide media exposure, terrorist organizations may be tempted to use hackers to spread their political messages or manifestos by hacking Web pages of particular governments or political organizations.

A perfect example was the recent violation of the Web page of the Indonesian Ministry of Foreign Affairs by

Portuguese hackers. Their goal was to call the attention of "Internauts" to the situation of East Timor. The introductory message of the page was modified twice, on February 10 and February 17, 1997, with sentences like "Welcome to the Fascist Republic of Indonesia" and an unflattering picture of the Minister of Foreign Affairs, Ali Abdullah Alatas. Recently, other hackers' targets have included the NASA, the CIA, whose site reproduced the phrase "Central Stupidity Agency", the U.S. Department of Justice, the FBI and the NCAA, whose page showed racial slurs. Moreover, in the United Kingdom the Web page of the Labour Party has been made ridiculous with links to sites which had nothing to do with British politics.[6] Hackers have also targeted commercial enterprises which use the Internet to advertise their products such as the Kriegsman Fur Company. In November 1996, hackers posted messages against the fur trade on its Web site.[7]

As these examples suggest, the potential for terrorist activities in terms of publicity are enormous but the main problem is to contact and persuade hackers to work for the organization. A possible first step would be to prepare a sociological profile of hackers although the task is quite complicated as the published sources have mostly been concerned with an analysis of penetration techniques. Nevertheless, it is possible to say that hackers are usually male, between the ages of 17 and 30. Although they may have not been successful in academic studies, hackers are highly intelligent and knowledgeable in their fields. They do not perceive themselves as a real threat to society. According to one of them, "a hacker is someone that experiments with systems by playing with them and making them do what they were never intended to do.

Hacking is also about freedom of speech and freedom of access to information."[8] Most hackers are, or were, employed on computer related jobs where they have, or had, chances to monitor the development of software and hardware. For many hackers, hacking is their primary occupation in life.

Although their activities are essentially solitary, hackers usually have a minimal organizational structure. They often get together in clubs and, more importantly, through conferences and other social events which are advertised on the Net. During these meetings, hackers tend to invite guest speakers such as retired hackers or even academic and computer security specialists.[9] A perfect case in this sense [was] the…"Hacking in Progress" conference…in the Netherlands [in] August [1997] where hackers, passwords crackers, phone phreaks and programmers…gather[ed] in one location to build the largest open air Ethernet in the world. Throughout the conference there [were] live video and audio links to another hackers meeting in New York called "Beyond Hope."[10] Thanks to these on- and off-line events, hackers are able to create a world-wide networks of contacts which is useful for exchanging ideas and news.

The reasons for hacking are various; they range from personal satisfaction, amusement or pure curiosity. As the previous examples of hacked Web pages have shown, some hackers are concerned about certain causes such as human rights, self-determination, or animal protection. These concerns may provide a route by which terrorist groups could attract hackers to their cause. Terrorist recruiters are going to have to explore the computer underground before actually getting in contact with the hackers and convincing them that their knowledge and background can play an important role in their fight against a particular government or state. Hackers conferences and meetings are a perfect venue were recruiters could get directly in contact with hackers. Having successfully “hired” one or more hackers, the terrorist organization will have among its supporters somebody who can tap into a wider global network of hackers.

Professional Hackers and Terrorists. The previous section looked mainly at the possible employment of hackers by terrorist organizations to spread propaganda. In addition, hacking activities can play an essential role in carrying out illegal activities such as fund raising or attacking government digital infrastructures by penetrating and disrupting them.

Fund Raising. The scale of ongoing computer fraud and crime is notoriously hard to assess accurately. In the *Information Security Breaches Survey 1996*, produced by Britain’s Department of Trade and Industry, only 3 percent of respondents reported incidents of computer fraud, with a fraud of £650,000 being the largest single logical (non-physical) security breach reported. Another computer fraud survey conducted by PA Consulting Group in 1996, however, concluded that some £20 billion per annum is lost to UK businesses alone, accounting for up to 3.5 percent of turnover. The difficulty in arriving at reliable results in such surveys is exacerbated by the fact that more than 85 percent of computer fraud goes unreported as institutions seek to preserve their reputations for secure practice.

Nonetheless, it is evident that the proliferation of information technologies and networks in the international economy has opened up to terrorist organizations new avenues for illegal fund raising. Central banks, stock markets, and large finance institutions transfer among each other large amounts of money through systems such as CHIPS, SWIFT, and FEDWIRE in the United States. At the same time, most banks are shifting some of their activities from branches to direct banking thanks to computer-telephone integration which provides links between the telephone system and databases, or even to the Internet as in the cases of Britain's Royal Bank of Scotland and Prudential.[11] Customers expect absolute security from these institutions when they deposit money. The profitability of financial and commercial entities, or even their survival, is directly related to their ability to stay constantly online in order to attract customers 24 hours a day and to ensure secure methods of payments by credit cards or special schemes such as "digicash."

Terrorist organizations may consider this reliance of Western economies on information systems and networks as a lucrative source of funds. One approach would be to penetrate the information systems of a particular company and insert logic bombs or Trojan horses in order to demand a ransom. This scenario was recently described in *The Sunday Times* which reported that, since1993 City of London and New York financial institutions were attacked 40 times by sophisticated cyber criminals who were able to extort £400 million.[12] Terrorist organizations can benefit from the panicky response that many companies, especially small and medium size ones, have in the presence of computer viruses or other malicious codes. According to an anonymous computer virus writer, "people think it is a major catastrophe when they are hit by a virus”.[13] By playing on such misconceptions and threatening to leak the story to journalists and so damage customer confidence, terrorist organizations could extort significant sums. Alternatively, terrorist organizations may try to steal money directly by entering financial networks. The recent case of Vladimir Levin, the Russian young mathematician who diverted funds from Citibank, is a perfect example of this tactic.

Infrastructure Attacks. Although financing is an essential prerequisite of a terrorist organizations, the ultimate goal of their “cyber-activities” would be the disruption or destruction of information infrastructures including basic services such as power supply, police databases, social security transfers, medical networks, transportation signals, money transfers and telephone switching systems. Terrorist organizations may prefer to operate in cyberspace since the risks of capture are less than in case of physical operations in a hostile country. Another reason would be to hamper the confidence of investors and operators in the security of the infrastructure of a particular region. This aspect may prove extremely damaging for local authorities trying to attract foreign investors not only through tax breaks or incentives but also by promoting the reliability of their transport and telecommunications infrastructures.

The Need for Professional Hackers. The above-mentioned IW operations require an extensive knowledge of computer programming and networking. Moreover, when planning an IW attack, the terrorist organization will have to carry out detailed intelligence work concerning the targeted system, including nodal analysis. Through this examination the terrorist organization will assess the vulnerability of the targeted system and define penetration methods. In particular, the terrorist organization will have to assess the importance of certain systems according to the information they carry or hold, identify their weaknesses, and then prepare the appropriate software weapons.

Due to the complexity and sophistication of these operations, terrorist organizations may decide to "hire" a professional hacker or cracker. The problem of finding such an individual is not hard to solve. The end of the Cold War led to the dismantling of Eastern European intelligence agencies. Most of these government agencies had developed extensive capabilities to violate computer systems in order to steal political and economic information. Moreover, some of the Eastern European states had developed an extensive knowledge in writing malicious computer codes in order to harm West European and American information systems. Today, most of the intelligence agencies have laid off software and computer hardware specialists because of budget constraints and lack of operational roles.[14]

In addition, the economic crisis of many Eastern European countries, and Russia, has meant that many high technology departments or research centres have been closed leaving many scientists unemployed and technicians with unpaid salaries. Throughout the 1990s, moreover, many largeWestern corporations carried out major internal restructuring by firing many technicians. Finally, there are a lot of Third World students with advanced degrees in computer studies but who have not been able to use their knowledge and capabilities back in their own countries.[15]

In spite of the deep reservoir of expertise, the recruitment of computer specialists may be risky for a terrorist organization as it may expose them to penetration by police or security services. Although the same case can be made for the “hiring” of amateur hackers, the situation with the professional is more complex as it can threaten the actual survival of the terrorist organization. It may be difficult to conceive of a professional computer specialist becoming involved in terrorist activities on ideological grounds since his or nationality or cultural background are probably different from the terrorists. The professional, thus mainly motivated by financial gain, is more likely to decide to switch sides. Furthermore, the lack of computer expertise of some terrorist organizations may also prove to their disadvantage as they may recruit professionals who prove unable to actually carry out the planned IW operations.

In any case, the recruitment of professionals may not be enough for the terrorist organization to carry out IW attacks against certain organizations. It is possible that nodal analysis carried out prior to the attack may indicate that the insertion of a malicious code may require an “insider” from the targeted organization. In this case, the terrorist organization has to find the right person, in the right position and persuade them to take risks for the cause. That this is possible to do is demonstrated by a number of surveys concerning information intrusion inside companies that indicate the majority of problems are the result of wrongful employee actions.[16]

Terrorist Group Profiles

In order to ground the above discussion in empirical data, two very different types of sub-state organization are considered here—Gulf radical movements and the Provisional Irish Republican Army (PIRA). The Gulf groups, mostly movements opposing the Saudi Arabian regime, are representative of loosely organized, transnational Islamist-oriented movements that are becoming increasingly active in the Muslim world. Although these groups have their origins in long-standing opposition movements they are not well organized or highly structured. Their leaderships tend to be based outside the country in question and they appeal both to a domestic audience and to a diaspora in the West. The movements consider themselves very much in the early stages of rebellion and are concerned mainly with consciousness raising and propaganda operations. Some elements of these movements are engaged in a clandestine armed struggle but this aspect of their strategy is not yet highly developed.

PIRA, in contrast, is representative of the small number of highly professional underground "armies" which draw on a long tradition of paramilitary resistance to the metropolitan power. Although propaganda is vital for the PIRA, it has long passed the early revolutionary stage of consciousness raising and is actively engaged in a sustained armed struggle. PIRA self-consciously mirror images its strategy on those of a conventional state at war. Thus it raises "taxes" to fund its operations and adjusts its military strategy and targeting doctrine in line with Clausewitzean notions of the subordination of military means to political ends.

These two sample sub-state movements therefore have quite different requirements. IW techniques would serve different functions for the movements.

The Gulf and the Information Revolution

Governments in the states of the Gulf Cooperation Council (GCC) have been concerned for many years to control the flow of information to and from their citizens. The aim has been to protect their societies against “subversive” messages—both cultural and political. Opposition movements operating in the 1960s began to overcome these controls through the use of radio. Voice of Cairo broadcasts served as a rallying cry for a generation of Nasserite Arab nationalist activists. In Oman and Saudi Arabia this propaganda had an impact but revolutionary tendencies were ultimately suppressed by the authorities.

The information revolution of the 1980s and 1990s has left these states struggling to catch up. Until the emergence of satellite TV and the proliferation of cheap satellite dishes, the residents of the GCC states were fed a diet of bland and politically conservative programming by their state channels. Access to satellite TV has in recent years enabled residents of the GCC to view a variety of international and national channels. GCC governments have sought to control this access. One method has been to ban satellite dishes, a policy which is enforced in the breach in Saudi Arabia. Alternatively, as in Qatar, satellite stations are piped to cable subscribers, enabling the authorities to monitor and edit programming. More generally, Saudi finance in particular has been used to seize control of much of the Arabic satellite TV output, as it has the pan-Arab press. Saudi-owned companies such as Middle East Broadcasting Centre and Orbit TV have the resources to dominate the market and ensure that coverage of Saudi politics remains off the agenda.[17]

While satellite TV poses one sort of dilemma for the Gulf governments, interactive communications media such as faxes, e-mail, and the Internet pose a far harder problem. The Saudi Arabian government's information control machinery is struggling to keep abreast of the flood of new media. The Supreme Information Council, established in 1977, under Interior Minister Prince Nayef, supervises the work of a vast network of censors. They are quite effective at dealing with domestic and foreign publications as well as controlling public spaces inside the country such as mosques[18] but controlling the new electronic media poses a number of problems.

First, the connectivity of Saudi society is increasing rapidly as the economy modernises and as the populace becomes ever better educated.[19] In response to these needs, the Saudis are investing 4 billion in upgrading their telephone system and installing 1.5 million extra lines.

Second, the technical problems of monitoring Internet access amongst a large group of subscribers have not been solved. Although the Saudi government has promised Internet access to business users, at present access is limited to universities and hospitals where the activities of individual users can be monitored by systems administrators and security officials.

Third, the Saudi diaspora, consisting of students, business travellers and holidaymakers, now has regular and unfettered access to the communications networks of the West. Cyberspace is thus accessible to many Saudis at frequent intervals even if they cannot access it from inside the Kingdom.

Islamist Psychological Operations. A number of Islamist opposition movements have been quick to seize the opportunities provided by cyberspace. These movements draw on long traditions of opposition to the Al Saud but the urrent conflict was sparked off by the Gulf War and the invitation to Western troops to defend the Kingdom against Iraq. The key groups are Wahhabi dissidents, the very movements that have worked in alliance with Al Saud since the 18th century but who have at various times risen up against the "impurity" and "corruptness" of a regime that is perceived to have made too many compromises with the infidels.[20]

The three groups of most interest are: the Committee for the Defence of Legitimate Rights (CDLR), the Movement for Islamic Reform in Arabia (MIRA) and the Committee Against Corruption in Saudi Arabia (CACSA). All have leveraged communication technologies to ensure a psychological impact out of proportion to their size.

The CDLR was founded in May 1993. Its leading members had, in 1991 and 1992, issued a list of demands to King Fahd which demanded more Islamic domestic and foreign policies. Ignored by the monarch but encouraged by the level of informal support, the leaders of the movement hoped that the CDLR would be a vehicle through which pressure could be applied on the monarchy. Instead, the government cracked down on the dissidents, imprisoning some and sending others fleeing into exile. The most prominent, Dr

Muhammad al-Masari, set up office in London where he acted as a voluble spokesman for the movement. Although well funded from private sources, Masari never had as many supporters in the Kingdom as did certain radical clerics inside the Kingdom. Nonetheless, by exploiting communications technology he rapidly emerged as a major political force. His office faxed some 800 copies per week of a newsletter to the Kingdom where it was distributed widely. An Email service and Internet home page widened his audience.[21]

By 1995/6, Masari's influence had become so great that his presence in London threatened a serious rift in relations between the United Kingdom and Saudi Arabia as Riyadh demanded that he be silenced. The British government, foiled in its attempts to deport the dissident, has gone so far as to rewrite immigration laws specifically so that activists such as Masari can be deported. By late 1996 and early 1997 a combination of internal rivalries, financial problems, intense Saudi and British government pressure, combined with a series of injudicious statements to the international press, meant that the CDLR lost momentum. Nonetheless, in its short heyday, the CDLR had demonstrated the power of modern information technologies.

MIRA was formed in March 1996 after its director, Dr. Saad al-Faqih, split from Masari. Faqih, an original founding member of CDLR, had wanted to focus solely on Saudi Arabia and was concerned that Masari's links with more radical pan-Islamist movements were discrediting the cause. Even smaller and less well resourced than the CDLR, MIRA's proactive and sophisticated media strategy has made it a leading voice of the Saudi Islamist opposition and a leading source for the international news media. MIRA has a well constructed Internet homepage and distributes a weekly newsletter. Faqih has frequently cited plans to begin satellite TV broadcasts but so far has faced legal and financial problems which have prevented this.[22]

CACSA emerged recently on the Internet in the United States and, unlike MIRA and CDLR, does not promote any individual as its leader. Instead it claims to represent a Saudi technocratic and business elite in general. There is some evidence that the group is an outgrowth of Shiite opposition movements that were active in the early 1990s. This earlier movement, which called itself the Reform Movement after 1992, operated out of London and Washington from where it published an authoritative newsletter distributed by fax to Saudi Arabia. This group made its peace with the Saudi government in 1994 and agreed to cease its propaganda activities. Complaints have however emerged that the Saudi government has not kept its end of the agreement and CACSA may be the work of dissident Shiites.[23]

The common theme from an examination of the propaganda activities of all of these groups is the striking extent to which they have been able to leverage information technologies to circumvent Saudi government controls on information collection and dissemination. There are three key elements. First, a very small and poorly resourced group, if it is skilled in the use of communication technologies, can have a major propaganda impact both internationally and in the Kingdom. Second, the Saudi authorities have been unable to find technical or security methods of controlling new information channels. They have had to resort to using diplomatic influence and traditional foreign covert operations to disrupt the activities of groups such as the CDLR. Third, a key feature of the new technologies is that, unlike radio or TV, they are interactive. Opposition sympathisers in Saudi Arabia can use fax, phone, and Email to send information to opposition activists in exile. The activists can then package and redistribute this information from their safe haven. Opposition movements therefore become information providers which greatly enhances their credibility and influence.

The final point to note is that the groups mentioned above have not even begun to consider more advanced IW psychological operations. Offensive techniques such as spoofing official Saudi broadcasts and hacking into official Web sites have not yet been tried. Similarly, these groups have as yet shown no inclination to use a wider range of offensive IW or software warfare techniques. This may be because they do not yet understand what is possible but it is also because they are in the early stages of their campaigns and are focused on consciousness raising rather than on physical operations against the regime.

The two bomb attacks carried out by Saudi dissidents against US forces in 1995 and 1996 were likely carried out by militants inspired by the exile leaderships but with no direct connections to them.[24] The comparative levels of technological sophistication between the IT and media-literate exiles and the combat-experienced militants are, for now, quite different. It is clear, though that the dissidents running the IT-intensive propaganda campaigns could turn their hands to more disruptive IW attacks if they so desired.

The Irish Republican Armed Struggle

Today's Irish republicans trace their armed struggle against England back at least to the 17th century but their more direct roots lie in the Fenian movement of the late 19th century. This movement practised terrorism and guerrilla warfare against England until the independence of Eire. The current "Troubles" began in 1969 after a series of civil rights marches. The PIRA emerged in 1969 when it split from the "Official" IRA, which has adopted a class warfare form of struggle as opposed to the Provisional's concentration on revolutionary warfare.[25]

PIRA is a minority revolutionary movement with a hard core of perhaps 500 and several thousand sympathisers. In the past 20 years some 5,000 members have passed through its ranks,been imprisoned, or killed. The PIRA's political wing, Sinn Fein, is a legal party in British elections and Northern Ireland local politics. In 1983, its vote peaked at over 10 percent of the population of Northern Ireland or around 40 percent of the nationalist vote. In light of its small base of popular support, the movement has refrained from mass action such as strikes and demonstrations. Instead it has forged a dedicated and professional cadre of paramilitary operatives. Its strategy is to make the cost of "occupying" Northern Ireland unbearable for the British state so as to bring about a British withdrawal. According to the PIRA, this would result in Northern Ireland joining Eire and becoming a sovereign state.[26]

PIRA has two key problems in carrying out its campaign. First, it needs to fund its activities. Unlike the Saudi groups discussed above, individual supporters of the PIRA do not enjoy large amounts of disposable income. Instead, the organization must raise its funds either from supporters abroad, such as NORAID in the USA, or from the community. In the Province, PIRA raises funds from a range of legitimate businesses and illegal activities—running taxi services, contracting, controlling gambling rackets, bank robbery, and money laundering.

Second, it needs to select and implement a politico-military strategy that leverages its limited resources into politically and strategically significant damage to the British government. Over time, PIRA's military strategy has altered according to political and strategic circumstances. Its main focus has been on undermining the government of Northern Ireland by attacks on the security forces or targets linked to them. Its tactics have consisted mainly of ambushes and bombings, with a number of tactical variations on the theme. It has also sought to raise the costs of governance by hitting commercial targets, such as the city centre of Belfast. The problem for the PIRA has however been to create a sense of irresistibility. In order to raise the costs for Britain and to sustain morale among its supporters, it needs to demonstrate that, even though the struggle may take decades, it can continue to cause damage and disruption. It is in this area that there is the greatest potential for the application of IW techniques.

PIRA's Campaign Against the Mainland Infrastructure. Since the early 1990s, the PIRA leadership has adopted a revised targeting strategy which they hope will better achieve their goals. It has become clear that low-level violence in Northern Ireland is of little concern to the public or politicians in Britain. Similarly, it is evident that major outrages on the mainland, such as the bombings of pubs in the 1970s, serve mainly to strengthen the determination of Britain not to compromise. Instead, the PIRA have adopted a strategy of targeting the commercial and transport infrastructure of the mainland. This is in addition to targeting British military and political symbols on the mainland, but these have become less important targets over time.

This strategy has not aimed to cause casualties, although these are often a by-product. Instead, it aims at causing economic losses to commerce and the government and disruption to the general public. The campaign began in 1991 and used bombings, backed up by hoax calls, to hit shopping centres and the railway network. In the wake of the 1992 General Election campaign, large vehicle bombs devastated commercial targets in the City of London and badly damaged a key motorway flyover in north London. In 1993 a series of bombs targeted British Gas installations and an oil terminal. In April 1993 the largest bomb ever detonated in peacetime in London went off in the heart of London's financial district. The PIRA enthusiastically noted that this attack alone may have cost between £350 million and £2.5 billion in damage and lost business.[27] In 1994 the campaign continued, with small bombings of shopping centres and railways. In March 1994 an attack on Heathrow Airport demonstrated a commitment to hit high visibility targets.

Later in 1994 the PIRA agreed to a cease-fire in the hope of entering the negotiating process in Northern Ireland. This cease-fire, however, broke down, and in 1996 and 1997 the organization resumed its operations. Once again, attacks focused on the national infrastructure. In July 1996, police arrested seven terrorists who had planned to bomb a number of electrical sub stations around London. Had they succeeded, there would have been "serious and widespread loss of electricity to London and the South-East."[28] In the run up to the British General Election, on May 1, 1997, the PIRA carried out a coordinated campaign of small bombings and hoax calls targeted at the London rail network and the national motorway network. On April 3, for instance, the country's central motorway network was put out of action for a whole day. The Freight Transport Association estimated that the disruption had cost British industry £3.5 million.[29]

PIRA and IW. There is no open source evidence of the exploitation of IW techniques by the PIRA. Clearly, though, the group could make use of IW for both fund raising and targeting. As discussed above, the PIRA raises some of its funds from sources such as bank robberies and fraud. There would appear to be significant benefits for the PIRA in employing hackers just as they employ more traditional criminals—to raid banks for instance. There is no evidence that the PIRA has tapped into this potentially lucrative source of funds but their experience with more traditional forms of crime and fraud mean that they may well move into this area.

In terms of the military campaign, the PIRA's shift to targeting the UK transport and commercial infrastructure raises intriguing parallels with the work of strategic theorists who argue for coordinated attacks, including IW, on national infrastructures in order to hit the enemy state's centre of gravity.[30] The PIRA is using traditional methods (high explosive and incendiary devices delivered by covert operators) against a traditional target set (roads, railways, energy supplies, shopping centers, and financial institutions). It is correct in its assumption that such attacks on key points are effective in causing embarrassment and cost to the British government. What it does not yet appear to have considered, however, is the potential benefit of using software warfare techniques to simultaneously target the British NII.

Although the British NII is not as sophisticated and extensive as its US counterpart, and therefore less vulnerable to such attacks, considerable damage and disruption could be inflicted on a variety of targets. Moreover, these attacks could generally be carried out at less risk and at lower cost than the current operations. Current mainland operations require several trained and trusted operatives, supported by a covert network of transport routes, safe houses and weapons. These operations are therefore vulnerable at many points to surveillance and interception by the British authorities. A software warfare attack, in contrast, could be carried out by one or two specialists operating with minimal infrastructure from a safe haven abroad.

In spite of the potentially huge leverage that such an IW campaign could have, there are a number of reasons why the PIRA may be reluctant to adopt IW. First, it does not fit with the organizational culture and group self image of the movement. The Irish Republican movement places great store by, even glorifies in, physical violence. Overt, violent operations such as bombing fit this self image. Subtle software attacks do not, though this may change if the PIRA realises the amount of physical destruction that could be caused by attacking certain components of the NII.

Second, the sociological background of most PIRA leaders and activists is not conducive to use of IW. The educational profile of typical activists is limited and "professional" terrorist training has so far focused on skills such as bomb making, small arms and intelligence work. The latter area would be a particular problem since the PIRA's intelligence professionals would need educatingin nodal analysis. Nonetheless, the PIRA does employ a number of electronics experts who have become proficient in fighting a low level Electronic Warfare campaign against the British Army's surveillance and Explosive Ordnance Disposal (EOD) specialists.

Third, the PIRA places a very high value on operational security. A strictly compartmentalised cell structure was introduced in the 1970s in response to successful penetration by the British security forces. Active Service Units (ASU) operating on the mainland generally separate their operatives by function, for example reconnaissance, arms storage, safe house preparation, and attacks. Lateral communication between cells is minimal. This emphasis on security has made the PIRA much harder to penetrate in recent years. This mind set would make the PIRA very reluctant to employ freelance hackers and crackers, whether amateur or professional. The risks of interfacing with possibly penetrated hacking groups may well outweigh the benefits from using their skills to launch IW attacks.

Conclusions

This paper aimed to present the preliminary findings of an inter-disciplinary research project recently initiated at ICSA. The main intention was to demonstrate an approach rather than to derive detailed conclusions. Each section of the research outlined here needs to be fleshed out with further desk research, interviews, and surveys. This is being done through multiple channels, using the different skills and expertise of the principal researchers.

This paper has demonstrated that, to derive a useful threat assessment, it is necessary first, to understand network and NII vulnerabilities, second, to understand the community which has the skills to cause damage and, third, to understand the groups that may potentially use these skills for political and paramilitary purposes.

This paper draws a number of interesting preliminary conclusions. First, there exists a pool of knowledge and skilled personnel able and willing to carry out IW operations, ranging from propaganda to software warfare. Second, even authoritarian and wealthy states such as Saudi Arabia have been unable to respond effectively to opposition groups that make sophisticated use of modern communications methods. Third, Islamist opposition movements are making effective use of IW and are able thereby to leverage their limited resources to achieve a major impact. Fourth, although the potential impact of software warfare attacks on the NII by groups such as the PIRA could be highly disruptive and cost-effective, for reasons of organizational culture and operational security, they may be reluctant to go down this road.

[1] Walter Laqueur “Post-Modern Terrorism” *Foreign Affairs*, Vol. 75, No.5 (September-October 1996), p. 35.

[2] Psychological warfare is of course a much broader activity than purely being a subset of IW.

[3] The concept of software warfare has been developed by Squadron Leader Peter Emmet of Britain's Defence Evaluation and Research Agency. See "Information Mania—A New Manifestation of Gulf War Syndrome?" *The RUSI Journal*, (February 1996), pp.19-26.

[4] For a definition of these terms see Martin Libicki, *What is Information Warfare?* (Washington, DC: NDU Press, 1995), and recent British government definitions.

[5] Disruption is used here as a shorthand for any form of unauthorised activity in a system.

[6] "UK@Connected-Party Poopers-Security Hacking Used to be Almost Respectable," *Daily Telegraph*, December 24, 1996, available on http://www.infowar.com

[7] The original and modified version of these Web pages can be seen by visiting the sites of "2600 Magazine," the main publications for hackers at http: www.2600.com

[8] D. Denning, "Concerning Hackers Who Break into Computer Systems," paper presented at the 13th National Computer Security Conference, Washington, DC, October 1-4, 1990 available at http:www.eff.org/links2.html

[9] For a description of hacker conferences in Las Vegas or New York see W. Schwartau, "Cyber-Christ meets Lady Luck-July 22-24th, 1994" available at http://www.infowar.com

[10] "Dutch Hackers to Host August Hacking Conference" Newsbytes News Network, March 3rd, 1997 available at http://www.infowar.com

[11] M. MacLeod "Interface-New Face of Banking puts Customer Back in Charge," *Times*, April 16, 1997.

[12] "Insight: City Surrenders to £400m Gangs" *Sunday Times*, June 2, 1996.

[13] National Computer Security Association (NCSA), *1996 NCSA Virus Study*, p. 231.

[14] W. Madsen "Intelligence Agency Threat to Computer Security" *International Journal of Intelligence and Counter Intelligence*, Vol.6 No.5 (Winter 1993), pp. 413-443.

[15] P. E. Sakkas "Espionage and Sabotage in the Computer World" *International Journal of Intelligence and Counterintelligence*, Vol.5 No.2 (Summer 1995), pp. 162-171.

[16] *The British Information Security Breaches Survey 1996* confirmed the findings of the 1991 UN Commission on Criminal Justice survey of 3,000 sites in the United States, Canada, and Europe where by far the greatest security threat was posed by employees. The 1996 survey of U.S. corporate security directors by Carter & Katz also mirrors this trend in finding that "the primary threat came from full-time employees, followed by part-time and contract employees, with computer crackers (hackers) a close third."

[17] A. Rathmell, “Netwar in the Gulf,” *Jane’s Intelligence Review* (January 1997), pp. 29-32.

[18] Sermons at mosques have been used to attack the regime but the clerics in question have usually been rapidly removed. Nonetheless, the authorities have been unable to stem the widespread distribution of audio tapes of such sermons.

[19] C. B. Gabbard & G. S. Park, *The Information Revolution in the Arab World: Commercial, Cultural, and Political Dimensions* (Santa Monica, CA: RAND, 1995).

[20] A. Rathmell and Mustafa Alani, *Saudi Arabia: The Threat from Within, Special Report No.12* (London: Jane’s Information Group, 1996); R.H. Dekmejian, “The Rise of Political Islamism in Saudi Arabia,” *Middle East Journal*, Vol. 48, No. 4, (Autumn 1994), pp. 628-643.

[21] CDLR’s home page is at: http://www.ummah.org.uk/cdlr

[22] MIRA’s home page is at: http://www.miraserve.com/

[23] CACSA’s home page is at: http://www.saudhouse.com/

[24] “Four Saudis Held for Riyadh Blast,” *Arab News*, April 23, 1996.

[25] E. Moxon-Browne, “Terrorism in Northern Ireland: the case of the Provisional IRA,” in P. Wilkinson, ed., *Terrorism: British Perspectives* (Aldershot: Dartmouth Publishing, 1993).

[26] Two problems with this analysis are that, first the majority Protestant population of Northern Ireland do not want to withdraw from the United Kingdom and are determined to oppose the republicans by force; second, Sinn Fein’s objectives receive the support of just one per cent of the electorate of Eire.

[27] An Phoblacht/Republican News, April 29, 1993.

[28] “IRA Bomb Gang Plotted to Black Out London for Months,” *Evening Standard*, April 11, 1997.

[29] “IRA Bomb Threats Paralyse M-Ways,” *Guardian*, April 4, 1997.

[30] J. Warden, “The Enemy as a System,” *Airpower Journal*, Vol. 9, No. 1 (Spring 1995), pp. 40-55.

CHAPTER 19

INFORMATION WARFARE IN MULTILATERAL PEACE OPERATIONS:

A CASE STUDY OF SOMALIA

By
Rick Brennan and R. Evan Ellis

Introduction

The primary mission of the U.S. military will remain to fight and win the nation's wars; however, it must also be prepared to achieve success in a whole panoply of operations subsumed within the category of operations other than war (OOTW).

The current usage of the term "operations other than war" includes all military operations not associated with a military confrontation during times of war. However, often the line between "limited war," and OOTW is hard to define….[T]he imprecision of the term OOTW obscures the diverse nature of military operations subsumed within this categorization. For instance, the term OOTW includes such varied missions as show of force, attacks and raids, noncombatant evacuation operations, support for insurgencies and counterinsurgencies, peace enforcement, peacekeeping, emergency humanitarian assistance and disaster relief, nation assistance, counterdrug operations, combating terrorism, arms control and counter-proliferation, [and] support to domestic civil authorities.

The capabilities required for some of these missions may indeed be "lesser included cases" of what is needed for war. Other missions, however, may require new ways to think about integrating emerging technologies, organizational structures, and operational concepts to better prepare U.S. forces for the types of operations they are likely to confront in the future.…Thus, any analysis of information warfare as it relates to an OOTW must, by necessity, be tailored to the specific mission and environment within which U.S. forces must operate.…

Information Warfare in Peace Operations

Information warfare is a critical component of military operations during times of peace and war. During times of conflict, information war is used to degrade or counter enemy capabilities and exploit his vulnerabilities while, simultaneously, protecting our own. Recent technological advances are giving information warfare new meaning in terms of how much can be collected, known, analyzed, and transmitted, while creating new challenges for managing that information.

Doctrinally, information warfare is implemented on the battlefield through the command and control warfare (C2W) strategy contained in CJCS MOP 30. This guidance states that the objective of C2W is "to decapitate the enemy's command structure from its body of combat forces." Effective C2W is described as enabling the commander to seize the initiative by forcing the enemy into a reactive mode, while maintaining, protecting and/or enhancing the effectiveness of friendly C2. It combines the denial and influence of information, deception, disruption, and destruction to counter adversary C2 while simultaneously protecting friendly C2.

Operational security (OPSEC), psychological operations (PSYOP), military deception, Electronic Warfare (EW), and destruction are listed as the five principal military actions used to achieve these results, with intelligence and counterintelligence as supporting activities.

While this strategy for the use of information war served U.S. forces well during Operation Desert Shield/Storm, its warfighting focus may not be fully suitable for the conduct of peace operations. Recent U.S. military participation in multilateral peace operations and emergency humanitarian assistance operations have cast U.S. forces into potentially hostile situations where there is no enemy. In these operations, while there may not be an enemy, per se, U.S. forces are likely to receive armed opposition from one or more of the parties to the conflict—especially during the conduct of peace enforcement operations.…

Legitimacy as the Center of Gravity

For U.S. forces deployed as part of a multinational peace operation, the challenges implied by the mission revolve around complex conflicts over “information” (broadly defined)—a struggle not over territory, but over legitimacy and the right of one party to rule over another. In a very real sense, all participants are seeking to gain and maintain influence over the “hearts and minds” of the local populace while maintaining their own political will to persevere.…

Because of the nature of the peace operation environment, “legitimacy” should be viewed as the center of gravity for coalition forces participating in the operation. Legitimacy may be defined as a condition growing from the perception of a specific audience of the legality, morality, and correctness of a set actions. It is initially derived from the mandate authorizing and directing the conduct of operations. However, the perception of legitimacy can only be sustained with the U.S. public, U.S. forces, indigenous parties, and the international community if operations are conducted with scrupulous regard for international norms on the use of force and regard for humanitarian principles.…

At the strategic level, the greater the degree of international consensus concerning the specific goals, objectives, and methods to be employed, the greater amount of legitimacy the mission will enjoy. Fractures in the coalition over perceived changes in the mission can erode legitimacy and ultimately threaten the success of the operation. Also at the strategic level, legitimacy is reflected by the amount of domestic political support that the operation enjoys from the informed public and their elected representatives. Much of this legitimacy is gained through the implementation of a consistent information campaign designed to clearly communicate the administration’s policy through what some have called the use of “public diplomacy.”…

Legitimacy is also the center of gravity at the operational and tactical level—often manifested by the support and/or compliance received from the parties to the conflict. Everything that the peace operation forces do and say will have an affect on the perceived legitimacy of the operation. Thus, in the struggle for legitimacy, control and management of information is of paramount importance—a lesson that was amply learned during recent U.S. military operations in Somalia while deployed as part of the Unified Task Force (UNITAF) and the United Nations Operation in Somalia II (UNOSOM II).

A Concept of Information War

Information Warfare can be divided into the functional areas of perception management, information degradation or denial, and information exploitation. Perception management, in the context of a multilateral peace operation, seeks to manage the flow of information in order to gain and maintain legitimacy. It may involve activities designed to gain the willing support or compliance of politically relevant actors or segments of the population through the provision or tailoring of information. During the conduct of peace enforcement operations, the most effective perception management strategies are designed to manage information that supports the peace process and reinforce the perception that outside forces will remain impartial in the enforcement of the mandate.…

The second category of information war is information degradation and denial. Within the context of a peace operation, information degradation and denial operations may seek to disrupt or contain information flows between parties to the conflict who place themselves in opposition to the peace process and strategically or operationally relevant outside players who are operating in theater. This could, for example, include temporarily preventing forces in opposition to the peace process from exploiting the advanced telecommunications capabilities of the international media to disperse inflammatory anti-U.S./UN messages. Information degradation and denial operations may also seek to disrupt the flow of information between nodes in the organizational structure of non-complying parties to the conflict.…

Information exploitation represents the inverse of information degradation and denial. It is the use of information of all types to achieve strategic, operational, and tactical objectives. These operations may seek to gain near-total situational awareness over the actions and status of the intended audiences and/ or targets. Information exploitation should focus on the political, cultural, and economic factors that may condition non-combatant responses.…For each of these functional areas, information warfare in a peace operations environment can be discussed in terms of relevant U.S. capabilities and vulnerabilities, and the potential capabilities and vulnerabilities of one or more parties to a conflict. The discussion that follows will show that the required U.S. capabilities may not fully correspond to familiar information assets (i.e., ELINT, SIGINT) as traditionally employed. It will also demonstrate that opposition forces in a peace enforcement scenario may possess a variety of non-traditional IW assets which may prove effective against U.S. and coalition vulnerabilities.

Perception Management

Perception management directed at theater non-combatants and politically relevant actors outside the theater is commonly placed under the category “Psychological Warfare” but is far broader in scope. In its broadest connotation, all information warfare operations can be viewed as an attempt to influence the perception and resolve of other players and/or opponents. For the purposes of the present analysis, however, perception management will be analyzed as distinct from active or passive attacks on information infrastructures (information degradation and denial) and the active use of those information flows (information exploitation). Perception management, as employed herein, includes such activities as counter-will operations, agitation and propaganda aimed at foreign target audiences designed to achieve immediate operational or strategic objectives. Perception management also includes preparation and dissemination of public information, distributed for domestic consumption, relating to the goals and objectives of national policy and specific facts concerning an ongoing operation.

As demonstrated in Somalia, "counter-will" operations do not necessarily require a plethora of technological assets. This is because "low-tech" opposition is often able to exploit outside communication assets—such as those of the international press. Further, a lesser developed opposition forces may be able to exploit decentralized societal networks which do not rely on technology to disseminate information to shape perception management. Both means are highly effective and are relatively difficult to disrupt with counter-IW technology.…

Somali Perception Management Capabilities

Somali warlord Mohammed Farah Aideed recognized the value of information war and employed perception management even prior to the initiation of UNITAF and UNOSOM II. Aideed conducted counter-will operations in Somalia through a public relations campaign that included dissemination of statement and interviews to the international press. The Somali warlord may not have possessed a clear strategic blueprint of how these activities would affect the political will of coalition member nations to operate in Somalia, yet he clearly acted with a general intention of causing political problems for those coalition nations.

Even before the deployment of UNITAF, Aideed's rhetoric and actions attempted, in part, to delay, undercut, and shape the UN force which would ultimately be deployed to Somalia. In 1992, for example, Aideed released reports that Italian businessmen, with the collaboration of his factional rival ali Mahdi, had dumped toxic chemicals in Somalia. These disclosures were made in an attempt to preclude Italian involvement in the peacekeeping operation and to discredit ali Mahdi. The charge was aimed at both shaping the character of UN involvement in Somalia, as well as supporting Aideed's maneuvering for power in the new Somali government. Aideed made other statements through his broadcast facility at Radio Mogadishu and through the international press during the pre-UNITAF period which were intended to inhibit the decision to deploy a UN peacekeeping or peace enforcement mission in Somalia. These statements included allegations that a Russian…airliner with UN markings had delivered arms and money to ali Mahdi….None of these actions were novel in their objectives or in their execution, but all were illustrative of Aideed's ability and willingness to use information directed at specific targets to achieve specific results.

During UNOSOM II, Aideed organized and staged events for the international media's consumption. It was the presence of the media which was the key to the effect of these events, rather than the events themselves. Aideed held a 2,500-person anti-UNOSOM II rally in the vicinity of the K-4 Mogadishu hotel (at which the international press was staying) on the same day that rival ali Mahdi held a pro-UN rally in northern Mogadishu attended by 250,000 Somalis. Because Aideed's demonstration was staged outside the hotel at which virtually all of the international media detailed to Somalia were staying, his anti-UN demonstration received widespread coverage, while the pro-UN demonstration which was 100 × larger went uncovered….Imagery such as pro-Aideed demonstrators burning tires—and the headless body of a U.S. serviceman being dragged through the streets of Mogadishu—were pictures that were picked up and repeated by media across the United States. These pictures came to represent the essence of the Somali operation in the minds of Americans—and thus helped undermine support for the operation.

Media Exploitation

Because Aideed lacked the sophisticated information warfare capabilities of the U.S.-led coalition, he concentrated on ways to counter U.S. superiority and exploit its vulnerabilities. Although the USC-SNA possessed few technologically sophisticated assets for perception management, Aideed had direct access to the capabilities inherent within the international media covering Somalia. Aideed recognized CNN as the primary battleground for his campaign against UNITAF and UNOSOM II from the beginning, and focused on getting his story out to key members of the media. Aideed was able to successfully manipulate peace initiatives and ceasefires to deprive the international force of a political rationale to militarily oppose his political maneuverings.

Aideed appears to have recognized that a small group of media members who were in Somalia for the long term were the key to winning the desired coverage. The K-4 Hotel in Mogadishu, which served as primary lodging for virtually all members of the international media visiting Somalia, was located in a part of town dominated by Aideed's Habr Geidar clan. This situation was ideally situated for Aideed's media courtship. The stringers who came into town to cover an emerging crisis generally lacked the contacts or background to cover the story on their own and, therefore, obtained the primary story line from the long-term press cadre. By focusing on this small group of "long-termers," Aideed was able to exert significant influence over the manner in which the media reported events in Somalia.…

Low Technology

Aideed's success with word-of-mouth communications and relatively low-tech radio broadcasts demonstrates that the comparable utility of sophisticated equipment is a function of the nature of the society and the availability of receivers (televisions, computers, etc.) within it. In his communication with the Somali people, Aideed's use of the traditional "word of mouth" network was highly effective because the USC-SNA leadership understood the clan structure of Somali society and enjoyed a substantial amount of credibility. Moreover, Radio Mogadishu served as an effective mechanism for Aideed to transmit his message throughout the Mogadishu region—an area in which his Habr Geidar supporters were concentrated. More sophisticated methods would have been of dubious utility given the low literacy rates in Somalia and the scarcity of televisions, radios and computers.…

Disinformation, Agitation, and Propaganda

Aideed also achieved specific provocation through the use of disinformation. Aideed’s pronouncements included his accusations of UN neo-colonialism and violations of Somali sovereignty over Radio Mogadishu. He called Somali attention to the hiring of Kenyan workers by the UN to perform certain tasks—rather than local Somalis. He further used Radio Mogadishu to convey his Islamic appeals to Somali society through his expressed desire to build an Islamic state despite the “opposition of evangelical Western infidels who would defile Somali culture.” During the 5 June attacks on the Pakistani peacekeepers, Aideed used agitators to appeal to the Islamic nature of Pakistan not to respond by firing (back) at their Islamic brothers. The public utilization of the “Islamic card” also limited Egypt’s role in the conflict to some degree because of domestic political problems the Mubarak government was experiencing with Islamic groups such as the Moslem Brotherhood.…

Aideed’s ability to influence his own people played a critical role in his perception management campaign, not only because it enhanced his own leadership and control over fellow members of his Habr Geidar clan, but also because it gave him the power to stage seemingly spontaneous, populist events. Staged demonstrations supportive of Aideed and the causes he professed made the warlord appear, to western democratic audiences, to have the support of most of the Somali people. At the same time, these demonstrations suggested to audiences in coalition member states that the UN force was contravening the right of the Somali people to choose their political leaders, religion, and culture….

Aideed also staged anti-UNOSOM II demonstrations with English-language placards for Western cameras and successfully exploited domestic sensitivities to the charge of neo-colonialism and appearances that the UN had infringed upon Somalia's "sovereignty." On 28 June, Aideed told Somalis to resist a tactical relocation by U.S. troops, then informed the media (who witnessed only the resistance by non-combatants) that the UN was forcing refugees from their homes. The anti-UNOSOM II theme became particularly pronounced during the 5 June to 9 October period during which Aideed was on the run from UNOSOM II and attempting to buy political breathing room in the Western media before the U.S. Quick Reaction Force could apprehend him or destroy his militia command structure.

Aideed's escalation of violence in Somalia beginning with the 5 June 1993 ambush of Pakistani peacekeepers appears to have been a calculated effort to restore his political position in Somalia by undermining both the UN presence and the national reconciliation process. Indirectly, the increased level of violence helped to achieve this by exposing and exacerbating political fissures among coalition members regarding the objectives of the UN operation. Although Aideed probably did not have a strategic perception management plan per se, his rhetoric, staged demonstrations, and actions were consistently aimed at the international media to stir-up opposition to the operation within troop contributing nations of the coalition. Aideed’s tactics were also designed to stir-up Somali anger and, at the same time, appeal to Western sensitivities by creating the conditions whereby forces assigned to UNOSOM II would be placed in a position where there was a high probability that they would kill Somali civilians. For instance, during the 12 and 14 June ambush on Pakistani peacekeepers, Aideed’s gunmen surreptitiously fired into a Somali crowd in the presence of international press coverage in order to convey the impression that the Pakistanis were firing on non-combatants….Following the 3 October firefight with Task Force Ranger outside the Olympic Hotel in Mogadishu, the Somali men who had been killed were quickly removed from the street—leaving only the slain women and children for the purview of the international press the following day. The removal of all but women and children casualties from the streets was also done following the July 18 firefight outside the Digfer hospital.

Beyond the specific propaganda value of Aideed’s acts and escalations, maintaining the international press spotlight on Mogadishu helped cause the international community to see the UN mission as an intervention, rather than a humanitarian or peace operation. In the process, his actions drew attention away from the successful humanitarian relief and nation-building operations in the rest of Somalia….

U.S. Perception Management Capabilities

Because perception management operations are potentially global in scope, the U.S. must maintain the ability to affect the perceptions of the leadership of parties to a conflict, as well as their domestic and international support base. Success in this arena, however, will very likely be predicated on the ability of the U.S. to develop an information strategy that can gain and maintain a broad-base of domestic support while, at the same time, shaping the perceptions of its coalition partners and the broader international community. The struggle to shape in each of these four arenas represents distinct but interconnected challenges. The common denominator of each, however, is the struggle to maintain legitimacy while denying that to parties on opposition to the peace process.

The U.S. public has historically identified propaganda and disinformation campaigns with communist and authoritarian regimes. Consequently, perception management, is widely conceived as exemplary of the behavior that we struggle against in times of war, rather than a largely political tool whose moral character is prima facie neutral. Because American political culture equates democracy with unfettered public discourse, perception management is often regarded as anathema to our system of governance....

The U.S. government is thus at an inherent disadvantage in conducting perception management operations because its attempts to disseminate information are regarded skeptically by the American media. For instance, U.S. military attempts to restrict media access in Grenada, Panama, and Operation Desert Shield/Storm were widely criticized by the media because it limited their ability to collect information independent of that which was being provided by official sources....

Information Strategy

Although the U.S. faced systemic difficulties in conducting perception management operations in Somalia, it compounded this weakness by failing to employ a comprehensive national level information strategy for UNOSOM II. The greatest obstacle to implementing a cohesive perception management campaign was conflicting statements coming out of Washington, the U.S. Mission to the United Nations, and the United Nationsí Secretariat.…

Facing an opponent that lacked a coordinated perception management campaign, Aideed was able to manipulate the international media successfully—diminishing U.S. and coalition resolve to remain in Somalia. Despite efforts by the UN civil affairs to highlight UNOSOM II successes beyond Mogadishu, these efforts were not coordinated with independent initiatives by the administration. Further, the UN civil affairs lacked the assets and political significance to influence the press to cover those events which it knew about in advance. For instance, in the Northwest and the Lower Juba region, the UN was able to create conditions that led to successful localized disarmament, establishment of institutions of local governance, and cooperation with UNOSOM II by the Somali Salvation Democratic Front (SSDF). These successes were not widely recognized outside Somalia.…

To the extent that these activities received press coverage, they had little impact on the perception of the American public because they had not been consistently linked together as supportive as critical elements of a broader strategy. Indeed, the principal message sent to the American public by the Clinton administration was that U.S. involvement in Somalia had ended when UNITAF troops returned home in May, 1993. Following the widely publicized ceremony in which President Clinton welcomed the troops back onto U.S. soil, the public was given the impression that U.S. troops were no longer in theater. The “hunt for Aideed” and the subsequent infliction of substantial casualties against U.S. forces on October 3, 1993, shocked the American public which was not only unprepared for substantial U.S. casualties, but was widely unaware that the U.S. military was still in Somalia.…

Force Deployment as Perception Management

In part, to reassure the U.S. public that the deployment to Somalia under UNITAF would be a short-term operation, the force size and logistics structure were kept small by minimizing forces and equipment placed on the Time-Phased Force Deployment List (TPFDL). Equipment that was not considered mission essential for a temporary littoral operation was not sent. Further, in order to avoid creating visual impressions that U.S. forces were digging in for a long-term operation, supplies were not sent for billeting, hot meals, morale, welfare or recreation. With no information about how long the operation would last, rumors ran rampant through units. Soldiers became disillusioned by contradictions between perceptions of those timetables drawn from operations in Somalia and public statements made in Washington concerning the scope and duration of the operation. Across the board, troops reported morale problems from living in tents and eating MREs to support an image of a “short term” operation while their coalition counterparts who recognized that there could be a prolonged presence, erected buildings and ate hot meals.

Coordinating Perception Management Within the Coalition

…The coordination and exploitation of coalition perception management resources was also an important, but not fully realized component of the overall perception management campaign. Since many perception management programs are based upon sensitive intelligence sources and methods which cannot be shared with foreign governments, U.S. forces did fully coordinate and share these capabilities with coalition partners. While efforts were made to overcome some of these problems, they were never adequately resolved.…

Public Affairs

The lack of an information strategy undercut perception management operations at the tactical, as well as the strategic levels. Traditional techniques for disseminating public information—such as cultivating relationships with experienced reporters, and the nightly press briefings conducted by Joint Information Bureau (JIB) commander—proved effective during UNITAF.

In contrast to UNITAF, however, the PAO in UNOSOM II was under-resourced and worked at a distinct disadvantage because there was no national level information strategy. Public affairs was not recognized as a combat multiplier and an important perception management asset. Ironically, because the U.S. presence in UNOSOM II remained substantial and the mission expanded, the need for public affairs under the new operation was at least as important as during UNITAF. Indeed, while the stakes for the United States had arguably reduced very little, the U.S. substantially reduced its ability to manage public perceptions domestically or internationally. For example, while UNITAF had sixty public affairs officers on staff, UNOSOM II had only six. Thus, the challenge of managing press coverage during UNOSOM II was complicated by the low levels of PAO manpower and support equipment.

As a result of all these handicaps, the U.S. PAO was unable to monitor international press coverage and correct misinformation which was being reported. Indeed, because of inadequate staffing, PAO officers were largely confined to the UN headquarters building during UNOSOM II, and often lacked the information necessary to respond to press queries originating from on-the-scene coverage of media correspondents in the field….

The PAO also lacked transport assets adequate to take the press or the numerous visiting VIPs to theater locations—a practice that is useful for disseminating information about operational successes. Consequently, the media made their own arrangements with local Somali gang members, resulting in an international press corps largely confined to Mogadishu whose primary perspective was gained from the information they obtained from their Somali escorts and guides—many of whom sympathized with General Aideed. Thus, the initiative in the public affairs sector for the battle to gain and maintain legitimacy was seized by the USC-SNA and others who opposed the UN military presence in Somalia.

PSYOP

Problems in U.S. perception management capabilities extended to the ability to affect Somali, as well as U.S. audiences. On this front of the struggle for legitimacy, the capabilities brought to theater by PSYOP were critical for success. Under both UNITAF and UNOSOM II, the PSYOP mission was, in part, to induce the Somali people to support the coalition's effort to restore peace and order to the country. Under UNOSOM II, however, it was unable or prevented from doing so because lacked sufficient manpower, equipment, and logistical support to adequately conduct the operation. Although 80 PSYOP personnel were deployed to Somalia under UNITAF, this number was reduced to a total of 5 during UNOSOM II. In addition, critical pieces of equipment such as loudspeakers were in short supply even though they were in high-demand by unit commanders who needed to communicate with Somalis.…

Language

Somali is not a common language, nor has there been a requirement within DoD for a large pool of Somali linguists. Consequently, language capability was an operational shortcoming throughout the mission, but was perhaps felt most in those PSYOP units tasked with perception management activities. PSYOP was particularly challenged by the need for large numbers of Somali-language translators. DoD and contract translators were generally adequate, although not all were familiar with the myriad of Somali dialects. Translators hired in theater effectively supplemented the former, but their work product had to be more carefully monitored because of their background and clan affiliation.

Somali Perception Management Vulnerabilities

The nature of Aideed's perception management capabilities and efforts gave him very little control over how the information was framed or the specific means by which it was transmitted—limiting his ability to influence how the information was received and interpreted by its intended target audience. Despite his ability to portray himself to the media in a positive light, he was widely perceived by the media as a significant obstacle to achieving long-term peace in Somalia. Even though Aideed's perception management tactics were ultimately successful, the credibility of his attempts to cast the UN in a negative light was limited by his dependence on the international media to carry his message. Moreover, this success was further dependent upon the credibility accorded to it by the broader international audience to whom it was transmitted.

Asset Protection

Aideed's attempts to protect his physical perception management assets proved extremely vulnerable. In part, the humanitarian purpose of the operation precluded UNOSOM II from seizing or destroying these assets upon initially entering the country—although the force never lacked the military capability to do so. Once it became clear that Aideed was actively working to subvert UNOSOM II, and once United Nations Security Council Resolution (UNSCR) 837 provided authorization for military operations to be used against Aideed's USC-SNA organization, Radio Mogadishu became an obvious IW target. The 12 June destruction of Radio Mogadishu by the U.S. Quick Reaction Force (QRF) and the capture of its two primary relay sites eliminated Aideed's ability to directly broadcast messages to the Somali population, and increased his reliance on the international media for his perception management operations. Thereafter, the USC-SNA retained a limited ability to make short-range, clandestine radio broadcasts via remote transmitters.…

Clan Support

A second vulnerability of Aideed's perception management campaign was the level of support that he was able to maintain from his fellow Habr Geidar clan members. This vulnerability was accentuated by the losses inflicted on the Habr Geidar by the UNOSOM II forces. Initially there was broad support for Aideed's actions within the Habr Geidar. For instance, on June 12 and 14 Aideed directed that women and children be used as human shields during an attack on Pakistani peacekeepers. This created a media spectacle by forcing the Pakistani soldiers to fire on "civilians" while television and print journalists watched. However, as Habr Geidar casualties mounted during the June-October attacks, Aideed's clan became increasingly divided over his leadership and his continued opposition to the United Nations. Ironically, however, senior level policymakers within U.S. and the UN did not fully understand the dynamics of Habr Geidar support or how it could be exploited as an Aideed vulnerability. For instance, the UN did not recognize the extent to which the "hunt for Aideed" would galvanize the warlord's supporters.…

U.S. Perception Management Vulnerabilities

UN forces proved exceedingly vulnerable to Aideed's perception management tactics. These vulnerabilities stem from the fact that the United Nations was not organizationally or doctrinally prepared to counter Aideed's IW campaign. The combination of a non-combat environment with the initially high profile nature of the operation meant that a large number of reporters flooded into Somalia and bought security and guide services from Somali gangs who had previously focused on extorting money and supplies from relief agencies operating in the country. UNOSOM II thus had little control over what the press saw or where they went. U.S. public affairs efforts in the field and in Washington were forced to be reactive—allowing Aideed to frame the story as it originated in Mogadishu through his control over the venue. UNOSOM II lacked both the strategy and resources to disrupt the decentralized disinformation capabilities afforded to Aideed and other clan leaders.

As with the PAO, PSYOP under UNOSOM II was inadequately manned and supported to accomplish the significantly larger mission assigned to it. UN civil affairs radio and newspaper assets were not available for PSYOP purposes, placing U.S. information dissemination and counter-disinformation capabilities at a disadvantage to Aideed who initially had control of Radio Mogadishu, and then later continued with his clandestine transmissions. Even where information could be disseminated to Somalis, the U.S. was far less intimately familiar with the Somali people and its culture than were leaders of the Somali clan leaders—making the U.S. message relatively less effective….

Information Degradation and Denial

As noted earlier, peace enforcement operations differ from warfighting in that success is measured through the attainment of political, economic, and humanitarian objectives, not the defeat of an adversary. Nonetheless, it must be recognized that in such operations, all sides will seek to deny information to the others. Moreover, one or more groups may deliberately target or seek to degrade U.S. information nodes or portions of its C4I2 infrastructure. Similarly, U.S. forces must anticipate and plan for occasions where it may be necessary to pursue the degradation of the information infrastructure of one or more of the parties to the conflict….

In Somalia, each side sought to achieve comparative advantage from those resources at its disposal, but in the realm of information degradation and denial, it was the relatively low-tech Somalis who were able to define the technological intensity of the battlefield more to their own benefit. Both the political objectives of UNOSOM II (nation building) and the lack of a Somali militia C4I2 technology infrastructure to disrupt, decreased the utility of such sophisticated U.S. counter-C4I2 assets as PGMs or wide-area jammers. While the Somalis were not able to disrupt the U.S. C4I2 infrastructure, they were able to deny the coalition intelligence concerning their movements and intentions by deciding not to utilize available electronic C4I2 assets which would have been vulnerable to interception.

Somali Information Degradation and Denial Capabilities

In Somalia, Aideed and Morgan were able to use comparably low-tech means to deny tactical intelligence to UN forces, while securing their own information infrastructures against disruption. Aideed never made serious attempts to disrupt technology-based information exploitation assets. There was no evidence of traditional electronic warfare by opposition force such as anti-radar or anti-communications operations. In addition, there were no discernible efforts to gain computer infiltration….

While Aideed did not conduct traditional counter-C4I2 operations against UN information warfare assets, he utilized low-tech techniques to deny information for coalition forces. With respect to active information denial, for example, Aideed cut off the flow of information to coalition forces from the Somali population by escalating violence and increasing the level of polarization within Somali society. By escalating the level of violence, Aideed intimidated coalition members from actively patrolling Mogadishu and obtaining a first-hand assessment of the changing mood of the population….

Aideed's information denial also encompassed the passive domain of operational security. His reliance on word-of-mouth information dissemination helped to reduce the utility of U.S. electronic information warfare assets. Both Aideed and Morgan curtailed their use of radio communication once they surmised that their message traffic was being monitored. This simple cessation of communication by radio dramatically reduced the ability of the U.S. to monitor the activities and intentions of each warlord.

Somali warlords also used the cover of civilians to disguise the movements of weapons and troops from UN forces. Women and children were often used by both General Aideed and General Morgan to transport weapons. In addition, civilian crowds were used as cover for staging attacks against UNOSOM II peacekeepers. In one situation, General Morgan infiltrated his soldiers into crowds in small groups to stage the February 1993 attack on Colonel Jess' troops in Kismayu—preventing U.S. aerial reconnaissance assets from spotting the movement until it was too late.

U.S. Information Degradation and Denial Capabilities

As noted above, U.S. QRF assets, including precision guided munitions, were able to effectively destroy Aideed's principal direct radio broadcast capability in Radio Mogadishu, although smaller mobile broadcast units continued clandestine operations throughout U.S. presence in UNOSOM II. Other U.S. information denial efforts, however, had little impact on the Somali warlords for a number of political and military reasons. U.S. radio jamming capabilities were ineffective or not employed against the sporadic and decentralized radio broadcasts made by USC-SNA militia members.

Potential counter-EW capabilities were also irrelevant against Aideed's"word of mouth" networks in Mogadishu. Operations in the territorially compressed urban area of Mogadishu made effective coordination of anti-UN actions possible through a system of couriers and through operating on "mission orders." Physical disruption of Radio Mogadishu was politically and diplomatically precluded until July 1993 by Aideed's strategic declaration of the station and a remote transmitter as weapons cantonment sites. Counter Command and Control operations were inhibited by coalition skittishness against proactive measures. While the low technology nature of Aideed's command and control network reduced the value of the destruction of equipment or facilities, the political requirement to provide advanced warning of attacks to avoid injuring non-combatants ensured that Aideed's command leadership had ample time to escape attack.…

The most important source of U.S. intelligence in Somalia was human intelligence—both from coalition forces and Somalis. Under UNITAF and UNOSOM II, the U.S. enjoyed good flows of information from both types of HUMINT, but would have benefited greatly from more. Somali clans proved hard to penetrate. Moreover, as suggested above, Aideed was effective in deterring greater cooperation by the local population.

Somali Information Degradation and Denial Vulnerabilities

Because the Somalis had few assets to degrade or deny coalition information flows, it is difficult to speak of specific vulnerabilities. Aideed's greatest weakness, of course, was that the U.S. and UNOSOM II communication network was free to function, limited only by difficulties with and shortcomings of the network itself. The USC-SNA harassment operations which limited UNOSOM II street patrols were vulnerable to the compensating intelligence of aerial and satellite reconnaissance assets—although many types of HUMINT which were lost could not be compensated for by photo reconnaissance and SIGINT. The information denial potential of harassing UN presence patrols could also be neutralized by the UN by sending more heavily armored or protected patrols into an area in which targeted information collection was required.

The central vulnerability of Aideed's clan-based kinship network (upon which he depended for tactical and strategic information denial) was the cohesion of the network itself. Because this network was an informal "reserve" rather than a disciplined military organization, cooperation with Aideed was an ongoing function of formal and informal persuasion, as well as the day-to-day calculus of personal interests by each member of Aideed's clan. The fact that the UN was helping to keep many of these clan members alive by feeding them and providing them with medical care and some employment, the massive casualties the clan was incurring in its struggles with UNOSOM II, and the superiority of the UNOSOM II force in terms of sheer military power all provided incentives for select members of the clan network to cooperate with the UN….After August 1993, however, information and assistance from USC-SNA clan-members trailed off as Aideed resorted to murder and mutilation to purge suspected USC-SNA "traitors."…

U.S. Information Degradation and Denial Vulnerabilities

Once the U.S. made the explicit decision to disrupt the USC-SNA command structure, it was, in general, highly effective in doing so. Although the QRF was able to take out the majority of Aideed's C2I nodes with the 12 July attack on Aideed's Abdi House headquarters and subsequent operations, the decentralized nature of Aideed's operations and the kinship basis of the USC-SNA militia network made it resistant to traditional counter-C2I and counter-organization tactics below the upper command level.

The primary vulnerabilities of the U.S. information degradation and denial capabilities were in the high visibility of the force required by the nature of the operation, the shortage of Somali-language translators, the repetition of standard procedures in presence patrols and other operations, and the ubiquity of the international media in Mogadishu….

The intentionally high profile of the UN force made its location and actions relatively transparent to Somalis. Because UNOSOM II was ostensibly a humanitarian operation, the troop contributing countries conducted presence patrols, cordon and search operations, weapons searches, and operations designed to support and assist NGOs, PVOs, and UN humanitarian agencies. During the conduct of these operations, a premium was placed on active interaction with the Somali population….Thus, even while operational planning could be conducted with relative security, UNOSOM II movements were highly visible to Somalis. UNOSOM II actions against the USC-SNA could be transmitted quickly, even by shouts, cowbells, and the "word-of-mouth" network to rally a crowd against UN positions.

The lack of Somali-language translators in the UN force required employment of local Somalis for translator duties. Because some of these translators had ties to Aideed's Habr Geidar clan, operations security was, to some degree, compromised. Operations security was also compromised by the repetitive nature evidenced in the conduct of operations. When conducting raids against suspected USC-SNA leadership hideouts, for example, a standard routine for force insertion and helicopter support was employed….

The presence of hundreds of members of the international media throughout Somalia also made it difficult to deny information on UNOSOM II or QRF actions to the USC-SNA. The humanitarian nature of the operation and the multinational nature of the coalition precluded the imposition of restrictions on press travel. Members of the media contracted with local Somali gang members for guide services, transportation, and protection, and were thus relatively unfettered in their movements throughout Somalia. Reporters on the scene during clashes between Somalis and UNOSOM II forces used satellite links to the INTELESAT system to make live broadcasts, providing the USC-SNA leadership with a de facto command and control network.

Information Exploitation

The dramatic differences between UN and opposition force information infrastructures show how information exploitation can be equally successful utilizing entirely different types of assets and operational concepts. They also show how the evaluation of information exploitation capabilities of an opposition force through the standards of the blue force architecture can produce devastating miscalculations.

In a broad sense, information exploitation consists of more than data collection, processing, and transmission; it also includes learning and adaptation. Under UNITAF, U.S. contact with the Somali population and superiority in information collection and dissemination techniques ensured that the U.S. learned and adapted faster than its principal militia opponents. However, during UNOSOM II, the preponderance of U.S. forces were precluded from conducting routine operations in Mogadishu, depriving them of opportunities for continued learning. During the same period, General Aideed continued to learn and adapt his operations to more effectively counter the larger and more technologically advanced UN force.

Somali Information Exploitation Capabilities

From a C4I2 standpoint, the most technologically sophisticated forces in theater were not those of General Aideed, but those of the U.S.-trained warlord, General Hersi Morgan. During UNITAF, Morgan used Motorola cellular phones with scramblers and channel jumping capabilities to coordinate operations with his forces. As noted previously, Morgan combined these communications with Maoist-style infiltration tactics to inflict a humiliating defeat on the forces of Colonel Omar Jess in the February 1993 battle between the two warlords in Kismayu. U.S. counterintelligence was aware of Morgan's cellular phones, scramblers, and channel-jumping capabilities and brought sophisticated electronic capabilities to theater in order to effectively monitor all his communications. General Morgan, perhaps realizing his technological vulnerability to U.S. counter-measures, never utilized his channel-jumping capabilities and eventually stopped using cellular phones altogether.

General Aideed's…most technologically sophisticated C4I2 assets were mobile, short-range AM-band radio transmitters and receivers. Although the U.S. possessed the capability to monitor these AM-band communications, Aideed ceased to employ these assets as a part of tactical adaptations made in response to being operationally stymied several times by UNITAF. Aideed's tactical intelligence gathering appear to have centered on unassisted visual observation of UN forces and their movements from rooftops and other vantage points, and through reports from militia members and sympathizers on the streets of Mogadishu. Once the information was gathered, it was relayed to Aideed by signals sent through such low-technology devices such as couriers and cowbells.

Some of Aideed's operational intelligence appears to have come from Somali workers and translators employed in support of UNOSOM II. Substantial information was also made available to Aideed by certain coalition members and sympathetic UN/NGO/PVO civilian workers....

Broadcast reports from the media were another source of tactical, operational, and strategic intelligence for groups and factions opposed to the UN operation. Ironically, televised news was perhaps the most valuable information exploitation asset in Somalia for all of the warlords. International media coverage of Somalia, and reaction to events in coalition capitols, provided Aideed and other Somali players with a wealth of timely information on the capabilities, intentions, and political will of coalition forces—information they could not otherwise have obtained....Media pictures provided accurate information about the general size, armament, and location of forces arrayed against him. It even provided coverage of changes in unit capabilities. For instance, on June 9, CNN reported the arrival of four AC-130 Spectre gunships, informing Aideed of new combat assets that was likely to be used by the coalition....

U.S. Information Exploitation Capabilities

Ironically, coalition technical information exploitation assets complimented those of Aideed's forces in many ways. UNITAF and UNOSOM II lacked assets in Aideed's areas of strength, but possessed capabilities for real time observation and communication that he lacked. The U.S. C4I2 system worked well in many ways to serve the force. U.S. assets included AC-130 Spectre gunships and OH-58D light observation helicopters. These were supplemented by somewhat less capable Italian and Canadian UH-1 utility helicopters with FLIR technology which greatly assisted in night reconnaissance. Search teams provided good ground and air reconnaissance for important convoys. When possible, military intelligence (MI) teams swept targets for non-combatants prior to aerial strikes.

Technology and Communications

Although intra-coalition communications capabilities were hindered by delays in implementing the satellite-based UN system and by a lack of direct coordination between national contingents, U.S. radio assets and GPS navigation equipment generally provided effective command and control. As noted above, U.S. radio equipment was able to successfully monitor the radio transmissions of General Aideed and the cell phone traffic from General Morgan's forces until each warlord stopped using technology-based communication assets….At the strategic level, CNN was ironically a good source of intelligence for U.S. forces as well as Aideed. Some of the most timely information received at the higher command echelons came through CNN. As one J-2 officer noted, mechanically it took time to receive general intelligence through the military command structure, while the press could link a commander straight to events.

HUMINT

U.S. technical capabilities were complimented by an abundance of human intelligence—albeit not enough. Indeed, it was estimated that 75 percent of usable intelligence in Somalia came from HUMINT sources. Although the relative isolation of U.S. Marines from Somalis under UNITAF and the paucity of Somali language translators under both operations hindered information flows, the daily contacts between U.S./UN forces and Somalis provided Commanders a wealth of information concerning potential hostility among Somalis toward the force. In some instances, Somalis working for or in contact with the force tipped off local commanders concerning hostile actions that were planned against them.…

At the low-tech end of the spectrum, the locally hired Somali translators were a critical link in the U.S. intelligence network. From the command level to the NCOs interviewed by the U.S. Army Historian's Office, intelligence specialists reiterate that they could not have functioned without these translators. In many ways, human translators provided capabilities that computers or non-Somali linguists could not have replicated. The translators not only facilitated verbal and written communication with Somalis and decoded intercepted messages, but also served as guides, reading signs of danger in neighborhoods or identifying which subclan dominated the area. The translators also picked up on cultural cues, such as reading body language and assessing whether the subject was lying.…

Somali Information Exploitation Vulnerabilities

The primary protection for the indigenous technical assets of Aideed's command and control network came from the emphasis of the UNITAF and UNOSOM II mission on support for humanitarian relief efforts. Prior to the passage of UNSCR 837 on 6 June 1993, these operations were not explicitly targeted at subduing a specific opponent. Because the purpose of UNOSOM II extended to supporting Somali nation building efforts, suppression or destruction of the Somali communication infrastructure was not conducive to the achievement of UNOSOM II goals. Aideed's information assets were protected because of the overlap between his military C2 network and the rudimentary Somali communications infrastructure.

The larger international political context of the UNITAF and UNOSOM II operations also indirectly provided a security umbrella for Aideed's communications network. The political requirement that UN forces had to provide a warning before initiating an attack on targets that had the potential to be occupied by non-combatants was perceived as necessary to preserve the legitimacy of the operation. The humanitarian basis of the operation similarly would have made it difficult to restrict the freedom of action of civilian relief workers or the international media....

The low level of reliance by Aideed on technology-based assets for command and control protected the overall functionality of the USC-SNA C4I2 infrastructure. Although the 12 July attack on Abdi House and subsequent counter-leader operations captured key USC-SNA leaders and forced others into hiding, the flexible nature of the kinship "information" and "command" network minimized the extent to which this undercut USC-SNA operational effectiveness. Because the USC-SNA had never relied heavily on a structured, technology-based C4I2 system, leaders in hiding could continue to obtain information from followers and organize attacks on the UNOSOM II force.…

Over the long-term, the informal, voluntary nature of the kinship system did present a vulnerability for Aideed from a command and control perspective. Because Aideed's command and control network depended on voluntary cooperation and obedience by his kinsmen, Aideed's attempts to protect his reputation within the clan and avert challenges to his leadership can also be considered as an indirect attempt to protect his command and control network—for without Habr Geidar compliance, the network itself would fade away.…

U.S. Information Exploitation Vulnerabilities

Although the U.S. had many valuable information exploitation capabilities in theater, it relied heavily on high-tech collection tools. Further, in an effort to reduce the size of the U.S. footprint in Somalia, lower-technology collection assets were substantially cut from the TPFDL. As a result, the CENTCOM JIC was forced to rely almost exclusively upon intelligence gained from imagery and SIGINT. These tools, while extremely useful in preparing intelligence estimates in times of war, proved less useful in a peace operations environment. For example, imagery was ineffective in monitoring militia activity in the southern regions of Somalia. In the border regions, aerial assets were generally ineffective in distinguishing between camel herders with personal firearms and militiamen crossing the border. In short, a system relying on SIGINT and satellite/aerial reconnaissance assets was not optimal against militias which did not look or act like conventional, organized military forces.

Technology

Given U.S. reliance on technology-based information warfare assets, it is surprising how little care was taken for asset protection. Despite the almost daily shelling of the UN compound containing critical U.S. C3I facilities under UNOSOM II, these assets were not placed in bunkers or hardened facilities. Moreover the use of unsecured channels for UNOSOM II logistics communication may have provided Aideed with information concerning preparations for UNOSOM II activities and thus facilitated the ambush of supply convoys—although Aideed's specific utilization of this information was never proven.

The U.S. compounded its over reliance on technology assets by projecting this technology-based capability base onto Aideed and Morgan. For instance, when Aideed and Morgan scaled back their electronic communications and began relying more exclusively on word-of-mouth coordination for operations, the ability of U.S. intelligence to anticipate their actions was significantly weakened. Moreover, when this occurred, U.S. intelligence assumed that the militias had ceased to communicate, when actually they had switched to other modes of communication.…

Culture and Language

Limited U.S. understanding of Somali culture also made the mission vulnerable to Somali tactical perception management operations. Although a number of Africa specialists deployed with the J-2 Joint Intelligence Cell (JIC), the personnel who filled out the J-2 unit for its deployment were generic intelligence specialists with almost no specific expertise in Somalia.…Consequently, many the clues providing evidence into the nature of the real struggle (between warlords for power in Mogadishu) were misinterpreted or overlooked.

The inadequacy of electronic surveillance techniques, assets, and human intelligence rendered U.S. forces extremely reliant on contact with local Somalis for warnings concerning militia action—and thus extremely vulnerable when that contact was not available or that information was not forthcoming. Without significant feedback as to Aideed's plans or the disposition of the population, UNOSOM II actions were repeatedly reactive to militia escalation or actions. After-action reports by both the UN and U.S. forces concur that widespread riots in Mogadishu were the worst expected challenge for UNOSOM II. The challenge to the 5 June AWSS inspection was not anticipated, nor was the use of RPG's and mortars against the UN compound. There was no warning from members of the population against the sniper ambush of Moroccans from the Digfer hospital on 17 June or the ambush of Task Force Ranger at the Olympic Hotel on 3 October, even though instigation of the population was used as part of the attacks in both cases.

HUMINT

Although HUMINT was extensively used during UNITAF, the focus on technology assets for intelligence collection precluded the recognition and utilization of all U.S. and coalition troops as human intelligence assets. The traditional focus on combat operations led troops to pass information to intelligence units only when incidents or conflicts occurred. In a peace operations environment, however, the essential elements of information are not the size, number, and disposition of "opposing forces" but, rather, the sometimes subtle changes in the political and social interactions within the society. While the best source for this type of information is the individual soldier, they did not generally view themselves as valuable collectors of information concerning levels of hostility among the population, the economic condition of villages, the condition of roads, and so forth—and consequently did not pass it along to the J-2….

Asset Availability

Because of the size and nature of the terrain covered by UNOSOM II, anticipation of opposition troop movements, ambushes, and the laying of command-detonated mines was sporadic at best. Although reconnaissance teams successfully provided intelligence protection for high priority convoys, the establishment of road blocks and attacks on vehicles from command-detonated mines continued as an escalating problem over the June-October 1993 period. It was not that U.S. assets were ineffective in identifying threats such as roadblocks, but that there were too few assets deployed to adequately monitor the expansive terrain and provide warning to U.S. and coalition-member troops in danger. Similarly with respect to Somali mine warfare, part of the problem was the lack of sophistication of Somali mines.

Homemade weapons built from plastic, C4, and a battery were not amenable to physical recognition as mines or detection by sensors.…

U.S. information exploitation capabilities under UNITAF and UNOSOM II were hampered in general by a lack of organizational assets. Although the U.S. contingent of UNITAF was, by far, more capable than the U.S. contingent deployed under UNOSOM II, a command decision was made to rely almost exclusively on satellite and aerial reconnaissance rather than ground assets.…Intelligence capabilities were further reduced by the failure of UNITAF to deploy with sufficient intelligence support equipment.…

Inter-Service Coordination

A lack of coordination between services within and across functional intelligence units also undercut U.S. C4I2 information exploitation capabilities. A lack of organizational experience as functional intelligence units proved to be another liability. Under UNITAF, for example, members of the Joint Intelligence Cell had not worked together prior to their assembly at Camp Pendleton for deployment to Somalia. Under UNITAF, the U.S. C4I2 system was also undermined by incomplete intelligence sharing between services. The 110th MI Battalion reported, for example, that information from the Marine CI teams was not reaching them. Further, when Army units were given the mission to assume control of operations in areas that had previously been controlled by Marines, applicable intelligence baselines needed for sustained operations were not transferred during the hand-off.…

Intra-Service Coordination

The lack of coordination also extended to interactions between intelligence and field units within the same service. Field commanders often asked for specific products (such as surveillance photographs), rather than questions (such as runway lengths) and failed to indicate whether they required the information to support a planned operation of their own or an anticipated act by a target. Consequently, the limited U.S. intelligence assets were over-tasked and the intelligence officers were precluded from optimally allocating assets to provide specific answers to specific questions, or supporting specific missions.…

Coordination Within the Coalition

Under UNOSOM, the coalition's C4I2 complex as a whole was also hampered by a lack of coordination across coalition members at all levels and between the coalition and the UN political leadership. Organizational and bureaucratic problems between the UN, host nations, and UNOSOM II precluded the exchange of important strategic information between them. At the UN Headquarters level, there was no political analysis or crisis response to military developments which changed the character of the operation from a de facto Chapter VI operation to a de facto Chapter VII one.…

At the operational level, the failures of coalition members to keep each other informed of their actions and developments in their AORs led to tactical blunders by other coalition members. The Italians, for example, failed to report to the UN when, in March 1993, they disestablished and destroyed the weapons in an ali-

Mahdi-controlled AWSS in the Italian AOR. Similarly, the coalition partners, including the Pakistanis, were not notified of the hostile USC-SNA reaction to UNOSOM II's announcement of the 5 June AWSS inspection; because of this, the Pakistanis argued, their troops supporting the inspection itself were left unprepared for the retaliations which had already been threatened by the SNA when the latter had been informed of the inspections on the prior day....

Real-time tactical coordination problems also cropped up between member forces. UNOSOM lacked the capabilities to monitor all radios in the coalition. Forces couldn't request support directly from each other when coming under fire, thus increasing coalition response times to ambushes. The Italians, for example, took hours to respond to the 5 June ambush of the Pakistanis and the 5 September ambush of a Nigerian convoy. Similar technical difficulties existed with respect to data sharing. Computer and video equipment of other coalition nations was often not compatible with that of U.S. forces, precluding the transfer of databases by electronic means....

Language

Language barriers compounded organizational obstacles to intra-coalition information flows. Coalition officers often had only marginal English language skills. Often foreign officers thus didn't have the language skills or familiarity with our intelligence techniques to know what questions to ask. While AOR commanders often received communication from other contingents or UNITAF /UNOSOM II headquarters, these messages were not always correctly interpreted and relations between coalitions were often strained.

Implications

Several important lessons can be derived from the above analysis with respect to the conduct of information warfare in future peace operations or other operations other than war:

1. There must be an overarching, realistic and fully integrated political, economic/humanitarian, military, and information strategy decided and articulated before any peace operation is initiated, whether it is UN or U.S. led.…

2. In the conduct of multinational peace operations, legitimacy must be recognized as the center of gravity for coalition forces. At the strategic, operational, and tactical level, legitimacy should be viewed as the center of gravity for the successful conduct of a peace operation.…

3. In peace operations, the “enemy” is anarchy, starvation, uncontrolled access to arms and munitions, the infliction of an unacceptable level of violence, and the absence of the institutions of governance—not a particular person or group. After the June 5 ambush of the Pakistani contingent in Mogadishu, the UN Security Council, drafted a Resolution calling for the apprehension and prosecution of individuals responsible for the attack on UN forces. The subsequent “hunt for Aideed” made the UN a participant in the conflict rather than an impartial arbitrator within a civil war.…

4. Public Affairs and PSYOP must be recognized as central components of an information warfare

system. Early integration of PSYOP and Public Affairs into the planning process and deployment of UNITAF were key to success. In combination with military intelligence, electronic warfare, and other U.S. capabilities, PSYOP and Public Affairs must be coordinated, integrated, de-conflicted and synergized to magnify U.S. Information Warfare capabilities.…

5. Multinational forces are strategically and operationally vulnerable to information war, especially in the area of perception management. Statements, information releases, and staged events for the press by leaders of parties that may be opposed to portions of the peace process may have both strategic and operational military implications. Agitation and propaganda conducted by parties opposed to the peace process may undermine long-term political support for the operation by raising the level of violence and producing local resistance to the UN operation.…

6. The lack of parallelism between U.S. information exploitation assets and those of low-tech “opposition forces” will reduce U.S. capability to conduct information degradation or denial operations. A system of information warfare optimized to combat an Information Age opponent may be sub-optimal for combating an agrarian age opponent.…The U.S. needs to anticipate that, in a peace operations environment, parties to the conflict will be at an inherent technological disadvantage to U.S. forces. The U.S. must anticipate that under such circumstances, leaders of parties in opposition

to the peace process may not attempt to conduct IW operations on our terms, but will attempt to counter U.S. technology-based capabilities with an IW campaign that exploits their connectivity to the indigenous population.…

7. The likely multinational nature of peace operations creates inherent difficulties for IW operations which must be anticipated and addressed. Complex C4I2 arrangements, dual lines of authority, and problems with coalition communications integration, for example, may be the largest obstacle to the optimization of traditional RSTA technologies or perception management operations within a coalition-led operation.…

8. Sufficient forces and capabilities should be deployed to accomplish the assigned mission. The desire to minimize U.S. force size in theater will be in constant competition with the desire to maximize operational effectiveness and limit the level of risk to American troops. While no American administration would deliberately deploy a force with inadequate information warfare capabilities for the task at hand, decisions designed to minimize the U.S. footprint may inadvertently result in limiting the type and amount of equipment and capabilities brought to theater.…

9. The international media is the most powerful offensive and defensive information warfare asset available to lesser-developed countries and/or parties to a conflict.…The media is

> structurally biased in both its on-site location and its need to find controversial or conflictual dimensions of an operation in order to “sell” to Western audiences. The U.S. must therefore recognize that passively providing access or relying on UN public affairs assets to represent the U.S. position will not be sufficient to ensure truthful, accurate, or even-handed coverage….

Concluding Thoughts

U.S. forces will continue to enjoy technological and numerical superiority over potential opposition in a peace operations environment. A preponderance of forces or technology, however, will not be decisive in this context because the asymmetries inherent in peace operations create new vulnerabilities for the United States while providing enhanced capabilities to opposing parties of the conflict. It can be expected that a future Aideed-type “opponent” will almost certainly seek to employ counter-will perception management tactics against the U.S. to undermine the legitimacy of the operation and attempt to shape the composition of the international force prior to its deployment, to limit the size and scope of its mission, and to restrict its explicit or tacit rules of engagement.

Media access will increasingly become an asset with a military value. During the conduct of a peace operation, it is likely that parties to the conflict will attempt to shape the media imagery by staging events with great visual appeal in locations and at times that allow correspondents to meet filing deadlines. Because of the multi-dimensional nature of a peace operations environment, attacks on the international coalition may be deliberately staged to discredit a rival in support of a domestic power struggle. Opponents may also attempt to stage counter-demonstrations or violence to detract media attention away from a domestic rival who is gaining positive coverage. As is often done in U.S. politics, opponents of the U.S. presence will facilitate access to those media members whose past record is most favorable to their perspective.…

With the proliferation of computers and Internet access in the developing world, greater employment of direct-access tactics can be expected, with the active assistance of the international media. This may include the establishment of a “HomePage” by a future Aideed, with daily interpretations or rebuttals of U.S. accounts of the operation.

The leaders of parties to a conflict in future peace operations may also become increasingly sophisticated in pursuing perception management operations among their own peoples. Although they may employ radio and telecommunication assets in doing so, it is most likely that they will seek to capitalize on the lack of telecommunications receivers among his countrymen and lower levels of literacy in the society to neutralize traditional U.S. technological advantages. Further, the leadership of parties to a conflict can be expected to play to U.S. unfamiliarity with the local language and culture by relying on credible and secure “word-of mouth” transmission networks and other traditional methods of communication with the population. Although such lines of communication may not be viable for fast-paced tactical operations, they can be reliably used to sew mistrust between local residents and the coalition forces.…

Future peace operations “opponents” can also be expected to use incremental changes in the type and amount of violence employed against the coalition as a tool to shape the will of the coalition to continue the fight. Leaders of parties to a conflict can, for example, be expected to escalate violence against weaker coalition members to splinter the weakest link of coalition commitment—as Aideed repeated did with USC-SNA attacks on the Pakistani brigades. Clan and faction leaders in certain cultures may also use women and children in attacks and establish defensive strong points in schools and hospitals to prevent coalition forces from mounting a coordinated and forcible response against their organization.

In the domain of information degradation and denial, opponents can be expected to render high-technology communications interception and battlefield monitoring capabilities relatively useless by failing to use high-tech communications and by failing to move in recognizable military formations across an identifiable battlefield. They can also be expected to wage relatively low tech attacks against critical, vulnerable nodes of the U.S. IW infrastructure. This may include physical assaults on interpreters or attempts to intimidate them by threatening locally residing family members. With the increasing use of sensors, the use of supporters to steal or disable sensors may become increasingly frequent.

In the domain of information exploitation, opponents can be expected to use their knowledge of the local culture and availability of human intelligence to compensate for their lack of technologically sophisticated C4I2 infrastructures. They can also be expected to leverage technology assets provided by the international media to increase their IW capability. For instance, satellite video feeds from on-site television network news will greatly assist parties conduct both battle damage assessment (BDA) and assessments of political reactions in host-nation capitols. Remote-site satellite transmissions will also increase the interactivity between actions on the ground and political debates in host-nation capitols, with events staged to influence key Congressional votes on an operation as they take place in Washington. Access to the Internet will also provide opponents with increasing level of information exploitation capabilities….Information warfare is a critical component of all military operations, but it is especially important for the United States in multinational peace operations and similar smaller-scale contingency operations that are commonly grouped within the category of operations other than war. If there is one glaring deficiency that can be easily corrected to limit U.S. vulnerability in this arena, it is the lack of a national information strategy. Just as it is necessary to have a National Military Strategy, it is now necessary to have a National Information Strategy, perhaps as a component of the Congressionally mandated National Security Strategy Document (NSSD)….

It is important to restate that no one organization in the U.S. government currently has responsibility for the totality of IW. Rather, various responsibilities and capabilities are diffused across staff sections, agencies, and departments—many of which have little opportunity or incentive to share information with each other. The result is an increasingly stovepiped organization that is resistant to coordination and integration. While this type of organizational structure may have been acceptable for information operations in the industrial age, it is a hindrance to the level of integration necessary for effective and efficient use of information warfare in the Information Age.…

In the radically changed environment our nation and armed forces face today, we cannot fail to more effectively leverage information to help promote and defend U.S. national interests. More effective use of the power of information in peace operations will significantly enhance the capabilities of U.S. forces to maintain the peace, contain the conflict, and accelerate the process of establishing peace and stability with the minimum loss of life.

CHAPTER 20

TARGET BOSNIA:

INTEGRATING INFORMATION ACTIVITIES IN PEACE OPERATIONS

By
Pascale Combelles Siegel

Introduction

With each day that passes drawing us further down the path from the Industrial to the Information Age, many officers are convinced that victory is no longer determined on the ground, but in media reporting. This is even more true in peace support operations (PSO) where the goal is not to conquer territory or defeat an enemy but to persuade parties in conflict (as well as the local populations) into a favored course of action.…

Following the signing on 14 December 1995 of the Dayton Peace Agreement, which put an end to a 4-year war in Bosnia-Herzegovina, the UN mandated NATO to oversee and enforce a durable ceasefire between the former belligerents. On 20 December 1995, a NATO-led multinational force called the Implementation Force (IFOR) started *Operation Joint Endeavour*. On 20 December 1996, a smaller NATO coalition called the Stabilization Force (SFOR) replaced IFOR. In *Operation Joint Guard*, SFOR received an 18-month mandate to oversee and enforce the ceasefire.

In Bosnia, IFOR and then SFOR ran an information campaign designed to "seize and maintain the initiative by imparting timely and effective information within the commander's intent. The term "information campaign" refers to the coordinated and synchronized use of different information activities within the command. The campaign had three components.

- A public information (PI) campaign designed to establish NATO's credibility with the international media to gain support from the contributing nations for the mission. Public Information Officers executed this mission.
- A psychological operations (PSYOP) campaign designed to influence the local population and its leaders in favor of IFOR troops and operations. PSYOP units (mainly American) undertook this aspect of the campaign.
- A Civil-Military Cooperation (CIMIC) information campaign designed to inform audiences about civil-military cooperation and to release information to aid the local populations. CIMIC elements (mainly U.S. Army) undertook this mission.

In this [study], information activities refers to the different components of the campaign, and information campaign refers to the coordination of the various elements. This terminology was adopted in part to avoid confusion with a new fashionable term: information operations. According to the *U.S. Army's*

Field Manual, *FM 100-6*, information operations refers to operations linking together public affairs, civil affairs, psychological operations, command and control warfare, and electronic warfare. Such all-encompassing information operations did not take place during NATO-led operations in Bosnia.

During the planning of *Operation Joint Endeavour*, NATO commanders and political leadership thought that information activities would make a critical contribution to mission accomplishment. In particular, they expected a successful public information campaign to contribute to building and preserving public support for the military operation.…

Information activities were also expected to help commanders communicate to the parties their intentions and might and to lead the local population to act friendly. During both the United Nations Protection Force (UNPROFOR) and NATO operations in Bosnia, major military operations were rare. On the other hand, IFOR (and later SFOR) often used information activities to deter the Bosnian factions from violating the military annex of the Dayton agreement and from attacking NATO troops. IFOR/SFOR also used information activities to convince the local population that a brighter future would await them if the Dayton agreement was fully complied with.

Before the NATO deployment began in December 1995, the stakes were particularly high for a successful information campaign. After the doomed UNPROFOR mission (widely perceived, especially in the United States, as a dramatic failure), a success or failure of the NATO mission was of utmost importance for the future of peacekeeping operations and for the credibility of collective security. As the first NATO ground military operation and largest UN operation ever, the success or failure of NATO operations in Bosnia-Herzegovina may determine the fate of UN and NATO peace operations for years to come. In consequence, it was of utmost importance that the mission be well explained to and well understood by the public at large and elite around the world.…

Political tensions in the United States also complicated the situation, with Congress reluctant to send U.S. ground forces to what many perceived as a quagmire in the making and the U.S. public always ambivalent about long-term commitments. Throughout the Dayton negotiation, partisans and opponents hotly debated whether U.S. ground troops should go to Bosnia as guarantor of the process. When the Clinton Administration decided in Fall 1995 that time was finally ripe for decisive political action in the region, it was well aware of the inherent dangers of its interventionist policy. To succeed, the policy had to be seen as successful and its merits needed to be well explained to the governing elite (especially in Congress) and the U.S. public.

Successful information activities were all the more important since propaganda had played a leading role in forging the war and justifying atrocities and crimes throughout the 4-year conflict. From the war’s outbreak, the media in former Yugoslavia mostly published and broadcast nationalist discourses, attacks and other general insults directed against other ethnic groups. It is not surprising that this led directly to horrible atrocities on battlefields and throughout the territory. Across Bosnia, the media became the loyal instruments of the factions' policies of war, ethnic purification, and atrocities….

Background on Operations in Bosnia

Operation Joint Endeavour began on 20 December 1995 after the Bosniac, Serb, and Croat factions (also called the Former Warring Factions, or FWF) agreed to a peace agreement that would end the 4-year-long war and ethnic cleansing. Representatives from the Republic of Bosnia-Herzegovina (represented by Alia Izetbegovic), the Bosno-Croat Federation, and Republika Srpska (Bosno-Serbs), along with the Presidents of Croatia (Fanjo Tudjman) and the Federal Republic of Yugoslavia (Slobodan Milosevic), referred to as the parties in the accord, negotiated the General Framework Agreement For Peace (GFAP) in Dayton, Ohio, and formally signed it in Paris on 14 December 1995. The accord is commonly referred to as the Dayton Peace Agreement (DPA)….

Summary of Main Responsibilities

The DPA lays down the responsibilities of the parties and the international community. The Bosniacs, Bosnian Croats, and Bosnian Serbs are mostly responsible for implementing the agreement. International organizations, with the notable exception of NATO, only have a facilitating role as supervisors and coordinators. According to the DPA, only NATO has the power to enforce the provisions of the agreement in case of non-compliance….

A key element in the international community's peace plan was the resurrection of Bosnia-Herzegovina as a unified country. At Dayton, the parties agreed to a single, democratic, and multi-ethnic Bosnia-Herzegovina (within the borders recognized by the international community in 1992). The new B-H is a federation made up of two entities: the Bosno-Croat Federation and the Republic of the Bosnian-Serbs (Republika Srpska)….

Overview of DPA Implementation

After 20 months of operations, the parties' compliance with the DPA goals remained low and inconsistent. From the start, the parties mainly complied with the military provisions of the agreement. They observed the ceasefire, respected the four mile wide Zone of Separation (ZOS) from each side of the Inter-Entity Boundary Line (IEBL), and agreed to the cantonment of their heavy weapons. They also allowed IFOR and then SFOR to monitor their weapons sites and troop movements. Finally, the parties granted Freedom of Movement to IFOR and the international community operating in B-H. Such level of compliance was achieved early in the operation, remained high during the IFOR operation, and continued under SFOR. However, as of fall 1997, the parties have not fully complied with the measures designed to achieve lasting security. First, although the three factions have completed the reduction of their forces to the agreed-upon level of a total 300,000, the OSCE-supervised arms reduction program has not been fully complied with, as the Bosnian Serbs have constantly underreported their heavy weapons holdings. Second, negotiations for establishing regional arms control balance in and around the Former Republic of Yugoslavia (FRY) have not begun….

As for the civilian aspects of the DPA, progress has been slow and inconsistent. Although the parties regularly stated their commitment to the DPA full implementation, they have multiplied the stumbling blocks on the road to reconciliation, leading many observers to believe that "Dayton implementation is but continuation [of the war] by other means."…There were three major obstacles in building national institutions:

- The main barrier to political implementation is minority fear. Serbs and Croats are afraid as minorities in Bosnia; Muslims are afraid as a minority in the region.…
- The Bosniacs and Bosnian Croats made limited progress in establishing the Federation institutions. As of fall 1997, few common institutions existed and those that did were barely functioning.…
- The Bosnian Serb leaders of Republika Srpska sought a weak central government, while the Bosniacs wanted a strong central government.…

Finally, democratization of institutions and minds proved a difficult process. The restructuring of police forces and judicial systems into democratic institutions did not occur. The IPTF training program affected only a minority of officers in the Federation and (as of July 1997) had not begun in the RS. Moreover, throughout a series of incidents, police forces displayed little professionalism, as well as lack of respect for democratic principles. According to several watchdogs in B-H, police forces were involved in harassment, intimidation, and black-marketeering. They acted as a tool of repression. The reform of the judicial system did not seem to have left the starting block. Likewise, democratization of the media in Bosnia-Herzegovina is slow. Most media across the country remained under tight control of the dominating factions and carried the messages that fit their political masters.…

The NATO Mandate

The United Nations Security Council Resolution 1031 (December 1995) mandated NATO to deploy an Implementation Force (IFOR) to Bosnia and Herzegovina "to help ensure compliance with the military provisions of the DPA."…Annex IA granted NATO a wide degree of authority to achieve its mission and established as a principle that IFOR had full authority to enforce the parties' compliance with Annex IA.…As a consequence, the parties agreed that to carry out its responsibilities, NATO has unimpeded right to observe, monitor, and inspect any forces, facility, or activity in B-H that it believes may have military capability. Refusal, interference, or denial by any party of this right "shall constitute a breach of this annex and the violating party shall be subject to military action by the IFOR, including the use of necessary force to ensure compliance with this annex." In conformity with these provisions, NATO commanders resorted to force to enforce the parties' compliance with Annex IA of the agreement.…

The Public Information Campaign

From early in the planning stage, NATO commanders expected information to play a critical role in the success of their operations in Bosnia-Herzegovina. As in any military endeavor, public support was central to mission accomplishment and Public Information (PI) was tasked with gaining and maintaining broad understanding for the mission.…

Organization

Upon deployment, IFOR established a large PI organization of about 90 persons designed to provide extensive PI presence wherever significant military activity was taking place. To that effect, IFOR established PI offices and press centers throughout theater.…

Concept of Operation

To effectively reach its target audiences, IFOR's message first needed to convince the reporters, who mediate the information. To convince reporters, IFOR PI needed to establish credibility. To be credible, IFOR PI needed to "tell the story as it is," to make as much information as possible easily available and to be ready to answer (as candidly as possible) reporters' questions. To ensure that its message be heard, IFOR adopted a proactive posture designed to stimulate media interest in its operations. The PI strategy was thus based on three principles: a proactive public information policy; a free and open media access policy; and complete, accurate, and timely reporting.…

Implications of PI Concept of Operation on C2

The IFOR PI strategy had important command and control implications. To provide complete, accurate, and timely information to the media, PI needed rapid information flow and thus had to be closely tied into operations. Specifically, PI needed to have close association with their commanders (to be kept abreast of their thinking), to be kept informed of plans and of operations and incidents as they unfolded (or as close as possible to that), and to be allowed to release information quickly to the press.

Commander Support

Following plans, most commanders gave full support to their PI teams and established close relations with their PIOs. For example, Admiral Lopez, USN, COMIFOR during summer and fall 1996, held his first and last daily meeting with Capt. Van Dyke, USN, the IFOR Chief PIO, or his deputy. COMARRC, LtGen Walker, UKA, usually chaired the daily ARRC information coordination group where information activities were considered.…Such an open and close relationship, however, did not seem to continue under SFOR. The SFOR CPIO had more limited access to his commander than his IFOR predecessor. The following changes in the CPIO/COMSFOR relationship occurred:

- The Chief PIO no longer enjoyed an open-door policy with his commander.
- COMSFOR no longer cultivated an informal relationship with his chief spokesman.
- Encounters between the CPIO and the COMSFOR were limited to formal morning meetings.

Relationship Between PI and Operational Staff Components

In addition, throughout the operation, commanders at IFOR and ARRC HQs ensured that the flow of information between PI and operations was adequate, allowing PI to gain complete and timely knowledge of current and future operations, even when classified. The highest integration occurred at IFOR HQ level, where the PI office had a liaison officer (LNO) permanently assigned to the Joint Operations Center (JOC)….

By providing a knowledge of plans and a clear understanding of HQ policy and thinking, these arrangements enabled IFOR PI to anticipate and prepare for incidents and difficult issues. They provided a rapid link between PI and operations, thus minimizing the likelihood that a reporter would break a story about NATO operations that PIOs were not aware of, and, thus, prepared for.

The Information Chain

The arrangements were likely to be tested when a sudden incident would occur and be reported in the media before IFOR was prepared to make a public statement. To avoid these situations, PI needed to be aware of operations and incidents as they unfolded (or as close to this as possible). This, however, constitutes a tough challenge. Reporting through a chain of command is time-consuming, as each authority level processes information before reporting to higher headquarters. It is an even more time-consuming process in a multinational operation where each layer might speak a different language, translate the incoming report, and process it in its own language before passing it up. Such a lengthy process cannot adequately support the PIO needs for timely delivery of accurate information. A typical information flow up a military chain of command simply cannot compete successfully with media reporting.

The challenge stems from the inherent imbalance between a journalist's ability to report on the spot and the military's need to process information before it passes it up the chain of command. First, journalists can relate any piece of news much faster than the military. Today's technology enables a journalist to broadcast an ongoing incident live (providing he or she is on the ground). While witnessing an incident, a journalist just needs to set up a satellite phone to break the news to his central offices. In a matter of minutes, the news may reach wide international audiences. By comparison, the military flow of information is much slower. Indeed, faced with the same incident, an officer will report the situation to his immediate higher headquarters. The process will be repeated until the information reaches a high enough level headquarters where the information can be cleared for public release. Second, a journalist may be asked to provide his "analysis," his personal interpretation of the situation to the best of his knowledge at the time of release. Military reporting, however, typically focuses on facts rather than impressions. Thus reporting might be delayed as attempts are made to confirm or complete the facts. Finally, the pressure to scoop the competition can lead to a situation where "being first is better than being right." Typically, it results in reporters going on air because something is happening, although it is unclear what is happening.…

Delegation of Authority and Confidence Between Headquarters

…Establishing trust and confidence, especially between the strategic level HQs in Belgium and the operational level (IFOR/SFOR HQ) was a challenge.

During Operation Deliberate Force, AFSOUTH and NATO/SHAPE experienced difficult relations. NATO HQ and SHAPE requested to clear all public announcements, including all daily press briefings and releases of combat camera imagery. Surprisingly, however, NATO, SHAPE, and AFSOUTH were able to dispose of Deliberate Force's legacy.

Under IFOR/SFOR, information release authority was delegated to the lowest possible level. COMIFOR/ COMSFOR had authority to release (or to delegate release authority to appropriate levels) all theater-operational information. In addition, IFOR/ SFOR PI were authorized to confirm news already obvious to the media without having to refer to higher headquarters. This provision greatly enhanced the PIs' ability to react quickly to fast-breaking news. Appropriate delegation of release authority allowed them to react in a timely fashion to fast-breaking news without interference from higher echelons.…

Public Information Activities

The PI strategy principles allowed IFOR and SFOR to provide a steady flow of information to journalists covering the operations. Aside from issuing guidance and producing SITREPS for higher and subordinate commands, IFOR and SFOR PI conducted the following activities:

- Everyday, IFOR/SFOR PI held a press briefing at 11:00 at the Sarajevo Holiday Inn. The briefing was the main venue by which the IFOR released information to the media.…

- Special briefings were organized at the IFOR press center when needed, most notably during VIP visits.
- IFOR/SFOR PI maintained informal relations with journalists. Before and after the daily briefing, journalists, spokesmen, and public information officers gathered in the CPIC hallway around a cup of coffee for informal chats and interviews.…
- IFOR/SFOR PI answered media queries. Any journalist could call the CPIC for information about operations.…
- IFOR/SFOR PI set up media opportunities for reporters and photographers. IFOR PI compiled regular lists of activities that reporters were welcome to attend.…
- IFOR PI produced and made available illustrative material for journalists, such as photographs of IFOR activities and maps. It is unclear whether SFOR continued this practice.
- IFOR/SFOR PI notified the press of incidents and significant events through press releases.

Limiting Factors

Several factors limited the effectiveness of IFOR/SFOR public information operations. For example, as in any deployment, PIO faced shortages of equipment and communications. Such shortfalls, however, did not significantly limit the PIO's ability to conduct its mission.

The SFOR HQ progressively marginalized the CPIO and other PI staff roles within the command group. This decreased the PIO's contribution to mission accomplishment. The strong support the commander had given the PI did not seem to survive the turnover to LANDCENT. From then on, the CPIO interactions with the commander were limited primarily to formal morning meetings.…

But throughout the mission, the major limitation stemmed from the multinational nature of the operation. Creating a truly multinational PI apparatus was a challenge. The IFOR OPLAN called for a multinational PI apparatus centered around the establishment of multinational sub-CPICs led by an officer of the largest contributing nation in a given sector. This structure, however, did not materialize.…

In addition, in a large coalition such as IFOR/SFOR, room existed for different PI concepts. These differences made it more difficult to run a concerted campaign. Although the PIOs in theater operated under NATO and SHAPE guidance, they also remained imbued with their own national doctrines and procedures. Even the three major contributors (the U.S., the UK, and France) had different approaches to public information operations.…

There also were frictions between IFOR and subordinate headquarters about the level and type of information that should be reported up the chain of command/chain of information. To be able to deliver complete, accurate, and timely information to the press, IFOR HQs PI expected fast, comprehensive, and accurate reporting from the subordinate commands. However, contingents did not always report as much information as IFOR felt it needed to handle media queries effectively. In some instances, contingents failed to report information that would reflect negatively on their attitudes or operations. In other cases, contingents failed to report on routine actions that they viewed as unimportant operationally. As a result, they did not report these “details” through the information chain.…

Conclusion

The main concepts of IFOR/SFOR PI operations served the commander’s needs and the public well. By providing complete, accurate, and timely information, IFOR/SFOR established credibility with the international media. Especially during IFOR operations, several internal arrangements supported the PI’s ability to provide this information. These arrangements included a functional chain of information, close relationship between the P10 and commander, and delegation of release authority. However, multinationality sometimes limited a fully effective implementation of these principles. Moreover, these principles were better attuned to the international media than to the local ones. This gap meant that the psychological operations campaign, specifically targeted at convincing the local populations, was all the more important.

Psychological Operations

NATO planners established the need for a campaign targeted at the local population of B-H and designed to shape attitudes and behavior in favor of IFOR (later SFOR) troops and operations. To carry out this task, IFOR’s primary tool was its psychological operations campaign, called the IFOR Information Campaign. Although an official NATO term, the term “psychological operations" was not used. Some NAC members did not want to be associated with a "psychological operations campaign."…"IFOR Information Campaign" seemed to ease these fears. However, there is little doubt that the "information campaign" was a psychological operations campaign. It was conducted by PSYOP forces and according to NATO's draft peace support psychological activities doctrine.

Organization

A Combined Joint Task Force…was responsible for implementing the NATO psychological operations campaign. Under IFOR, the task force was called the Combined Joint IFOR Information Campaign Task Force (CJIICTF). With SFOR operations (20 December 1996), the name changed to Combined Joint Information Campaign Task Force (CJICTF). Both task forces were directed by a U.S. Army Reserve Colonel, and were mainly composed of U.S. personnel and assets with supporting elements from France, Germany, and the United Kingdom.

The IFOR Structure

The Task Force featured centralized planning and management at headquarters level, and decentralized execution by subordinate elements from divisions down to battalions.…At the operational level, the CJHCTF had three elements:

- The headquarters was in charge of planning and managing the campaign.
- A PSYOP Task Force (POTF FWD) located in Sarajevo conceived and developed the products

to be disseminated throughout theater and operated five IFOR radio stations.

- The HOP staff located in Zagreb produced the weekly newspaper called The Herald of Peace. After a few months of operations, the HOP staff joined the rest of the Headquarters in Sarajevo.

At the tactical level, support elements in charge of product dissemination were attached at corps, division, brigade, and battalion levels. PSYOP, Support Elements (PSE) at division and brigade levels provided planning and execution expertise, while Tactical PSYOP Teams (TPTs) disseminated products and gathered feedback on the IIC effort.

The SFOR Structure

With the transition from IFOR to SFOR in December 1996, the PSYOP task force organization somewhat changed. Although the new CJICTF was still structured around a core U.S. element, the presence of foreign supporting elements increased notably.…

Concept of Operations

The PSYOP campaign was designed to influence the local populations and FWF to cooperate with NATO activities. To achieve these goals, the task force ran a multimedia campaign, albeit a limited one, and sought to use step-by-step psychological processes to entice attitudinal changes.

A Multimedia Campaign

The PSYOP campaign sought to reach the local population through a multimedia campaign relying mostly on NATO-owned assets. In the Bosnia context, where the factions tightly controlled the local media and used them to propagate their self-serving propaganda, IFOR/SFOR needed to circumvent the local media to effectively reach the local audiences. Also, in a country where people are accustomed to modem media and have relatively sophisticated expectations, the PSYOP campaign sought to take advantage of several venues to disseminate its message. To achieve these goals, NATO resorted to a variety of self-owned media:

- A newspaper. IFOR printed a weekly newspaper, *The Herald Of Peace*. This publication became a monthly paper, *The Herald Of Progress*, with SFOR.…
- A monthly youth magazine…*Mircko*,…designed to appeal to the teenage audience.…
- Radio stations. The number and location of the IFOR/SFOR radio stations varied throughout the operations.…These radios operated at least 18 hours a day with music, news bulletins, and messages.
- Television spots. As of March 1997, IFOR/SFOR had produced 51 television spots to be given to local stations throughout theater.
- Posters and handbills. More than 3 million posters and handbills were disseminated throughout theater between December 1995 and November 1997.

A Limited Campaign

The PSYOP task force was to abide by a number of limitations. First, the PSYOP task force was only allowed to run a limited campaign that relied on true and factual information. Second, the task force was under an obligation to always identify itself as the source of the information. It was forbidden to use disinformation or deception.…Third, the nature of this peace support operation also limited the nature of the message. Unlike in wartime, there were no declared enemies in B-H. Therefore, messages undermining the factions…were deemed inappropriate, even though the factions regularly stalled or prevented full implementation of the agreement they had signed.…

A Step-by-Step Psychological Process

Within these constraints, the PSYOP task force sought to use psychological processes to achieve attitudinal changes. According to Colonel Schoenhaus, commander of the (SFOR) CJICTF, the campaign "chose to expose the local populations to deliberate sequences of ideas selected for their potential psychological impact in a step-by-step process to create in the mind of the target audience an acceptable alternative course of action."

This process involved carefully selecting the messages. The CJHCTF had the latitude to select the facts it chose to release as it was not compelled to "tell the truth, the whole truth, and nothing but the truth." It therefore chose which and how much information to put forward, and how to argue its case. For example, an explanatory pamphlet on the Brcko arbitration decision released in March 1997 throughout Republika Srpska did not mention that the RS leadership had rejected the decision. In another example, the SFOR chief information officer insisted that a *Herald Of Peace* article on education should not quote a Bosnian Croat Minister explaining that children in territory under Croatian military control would be taught the Croatian version of Bosnia's history. The Chief Information Officer later explained that the PSYOP campaign was not in the business of informing, but in the business of convincing.…

Alteration to the Original Concept

The original concept of operation, described above, did not change much over the course of both IFOR and SFOR operations. Throughout, the campaign remained under the same limitations and sought to use step-by-step psychological processes to entice attitudinal change. The only major change resulted from the perceived lack of readership.…

Throughout the operations, IFOR and SFOR PSYOP campaigns were not adapted to the local populations' media consumption habits. The PSYOP campaigns relied primarily on printed material (newspaper, news magazines, and posters), while the Bosnians' preferred medium was television. In addition, few Bosnians read papers regularly because they are expensive, and tactical teams found that posters did not appeal much to this audience.…

Likewise, in the radio field, IFOR/SFOR radios transmitted on AM while most Bosnians listened to FM radios. These difficulties were compounded by the competition from local news outlets. Indeed, from the start of the operation, the CJHCTF found itself competing with the local media for visibility. According to a USIA survey released in April 1996, most Bosnians got their news from their local/ethnic media. In addition, they trusted these outlets most to get accurate news.…

In response to that challenge, the CJHCTF altered its original concept. In fall 1996, the CJIICTF began to rely on the domestic media to carry IFOR’s messages to the public. To avoid tampering with products by local journalists/editors, the CJHCTF provided the local media with finished products. The CJHCTF developed TV programs for local television stations to broadcast and provided local radio stations with music tapes accompanied by short messages. By the end of the IFOR mission, the CJIICTF also printed posters (ads) to be inserted in local newspapers. Resorting to local media allowed the CJHCTF to expand its coverage, and to insert its message into media which had a high level of credibility within the local populations. The SFOR CJICTF retained and expanded all these new means of disseminating the PSYOP message.

Psychological Operations Activities

The primary mission of IFOR and SFOR Psychological Operations was to deter armed resistance and hostile behavior against IFOR/SFOR troops and operations. The PSYOP campaign was primarily conceived as a force protection tool. First, by making NATO’s mandate and intentions clear to the local population and FWF, the IIC sought to prevent misunderstanding leading to unnecessary violence. Second, the IIC objective was to ensure broad compliance with the Dayton Peace Agreement and discourage the factions from interfering with IFOR/SFOR operations.…

As operations unfolded, the FWF complied, for the most part, with Annex IA of the DPA and the local population did not interfere or become openly hostile to the NATO troops. As a result, the CJIICTF began to promote themes designed to facilitate broader DPA implementation and to get the local population to support international community activities for a successful return to peace and reconciliation. The PSYOP campaign actively supported civilian agencies operating in B-H (mostly the OHR, the UNHCR, the UNMIBH, and the OSCE before and during the elections)….

SFOR Activities

With SFOR operations, the civilian themes component of the PSYOP campaign grew in importance. As General Crouch, USA, COMSFOR, determined that progress in the DPA civilian implementation was vital for successful mission accomplishment, the CJICTF was tasked with promoting democratic action, adherence to the rule of law, acceptance of returnees, and the ability of SFOR to enforce a secure environment in an even-handed manner. The CJICTF chose to underline themes with a slightly more aggressive approach than IFOR. The CJICTF viewed the people of Bosnia as the major proponents of change. By showing them how elected leaders should behave in a democratic country, the CJICTF hoped to raise the people's expectations toward their leaders, and ultimately, trigger major changes in the political landscape. For example, the CJICTF developed a series of products designed to explain how certain institutions (such as the military, the media, and the police) should behave in a democratic society. These products were designed to raise the population's expectations of their respective police and military forces. Likewise, the CJICTF developed a campaign in support of the elections motivating locals to vote for leaders "who will bring a brighter future."…

The Command and Control Situation

Political sensitivities not only made European nations reluctant to using PSYOP, but also complicated the command and control situation. From December 1995 to October 1997, U.S. PSYOP personnel (which formed the core of the CJHCTF) remained under national command and control. As a result of the 1984 National Security Decision Directive 130 (NSDD 130), the U.S. Department of Defense refused to place PSYOP forces under NATO command and control (C2)….The American refusal caused problems in everyday operations.…

Approval Process

The dual chain of command had practical effects, most notably in complicating the concepts and procedures for approving PSYOP products prior to dissemination. PSYOP products were developed and approved at theater level. In theory, the PSYOP task force headquarters developed the products in accordance with the NAC's approved themes and objectives and COMIFOR/COMSFOR approved the products before dissemination. In practice, the process was a little more complicated. Throughout the operations, various nations involved in the PSYOP effort retained review or approval authority. For example, German PSYOP forces, which developed the monthly youth magazine *Mircko*, had to send each issue back to Germany for a final review before dissemination. This review was established as Germany wanted to avoid any problem with its World War II legacy in the area of operations.…

Relations with the MNDs

Throughout both IFOR and SFOR operations, tensions existed between the multinational divisions and the PSYOP task force headquarters. The difficulty to balance theater and divisions requirements generated these tensions. Both IFOR and SFOR insisted that the PSYOP campaign was theater-wide. This approach allowed IFOR to run a unified campaign across theater.…

Consistency faced challenges, however, as divisions sought more freedom to conduct their own operations. From Joint Endeavour's opening days, various contingents attempted to run their own PSYOP activities. For example, the UK-led division acquired some printing equipment in spring 1996 to develop some products specific to its AOR. In MND (SE), Spanish and Italian contingents conducted PSYOP activities in support of their CIMIC operation. This tendency only increased with SFOR as non-U.S. forces decided to create or strengthen their PSYOP capabilities in Bosnia. Under SFOR, the UK-led MND (SW) published a magazine (*Mostovi*). In MND (SE), the French, German, Italian, and Spanish contingents all conducted PSYOP activities. As far as the author is aware, there was little coordination or synergy between these efforts and the CJICTF campaign.…

A Weak PSYOP Campaign

In addition to organizational problems, a number of factors undermined the effectiveness of the campaign. The most serious was discussed above—the very nature of a peace support operation. This meant that in Bosnia-

Herzegovina, the NATO PSYOP campaign could not take actions that might undermine the parties to the DPA even though these parties themselves were often the most significant obstacles to DPA implementation.…

Difficult Adaptation to the Cultural Environment

As in any other operation, the PSYOP community needed to adapt its message to its target audience. For its message to be effective, the PSYOP campaign needed to use arguments relevant to the local cultures and to present them in a way that would appeal to target audiences. This was difficult to achieve as the PSYOP campaign lacked regional experts and adequate resources to determine the populations' expectations.…

Working With International Organizations

…Supporting the international organizations was an unusual task. PSYOP forces rarely operate closely with international and non-governmental organizations. During Joint Endeavour and Joint Guard, however, supporting civilian organizations constituted a large part of the PSYOP work. But the CJICTF encountered many difficulties in establishing and maintaining fruitful relationships with international organizations.

A first challenge was to establish an effective PSYOP/civilian agencies interface for communicating requirements and capabilities between these organizations. Throughout the operations, the PSYOP task forces had limited access to the international organizations and little information about their operations.…

A second challenge stemmed from different civilian and military planning and action cycles. The military is generally more planning oriented than civilian organizations, while the latter deal more in the immediacy. Although many in the military seem to believe this derived from civilian incompetence, it relates far more to differing resource availability and missions.…

A final challenge consisted of developing a message that fit both the I0s and IFOR/SFOR needs. Each organization had its own agenda and priorities and these were not always in full accord.…

The process for developing and approving products that potentially affected the IOs' responsibilities thus left room for error and misunderstanding. Indeed, such products could easily contradict the civilian organizations' messages. It seems, however, that the civilian organizations did not pay much attention to this problem. Interviews conducted in March/April 1997 revealed that civilian organizations were not aware of most CJICTF products. Their attitude seemed to have less to do with the process, rather than with their views of the CJICTF campaign's effectiveness. OHR, UNHCR, and UNMIBH personnel commented to the author that they had little use for a campaign that was too weak to have any substantial impact.…

The Difficulty of Assessing PSYOP Effectiveness

Adaptation to the local environment was all the more difficult because PSYOP had difficulties assessing the campaign's impact. First, it is difficult to measure the real impact of any communication. Research shows that communication's impact is almost never direct. Establishing a direct link between a message and a specific attitude is therefore difficult. On top of these scientific limitations, the IFOR and SFOR PSYOP did not have adequate resources to conduct an effective assessment of their impact.…

Conclusion

PSYOP was entrusted with a vital mission in a difficult environment: provide an honest alternate viewpoint in a sea of local propaganda and disinformation to facilitate DPA implementation. However, three sets of factors limited the effectiveness of the PSYOP campaign. First, political sensitivities surrounding the use of PSYOP forces made it more difficult to run an effective, multinational PSYOP campaign. Second, the weak and conciliatory nature of the PSYOP message limited its potential impact on the local populations. The task forces' difficulties in adapting to the local culture and media habits further impaired the campaign. Finally, these shortcomings were all the more difficult to correct as PSYOP's assessment of its effort was at best limited.

CIMIC Information Activities

In addition to PI and PSYOP, IFOR and SFOR Civil-Military Cooperation (CIMIC) units were also tasked with conducting information activities. CIMIC, composed almost exclusively of U.S. Army reserve civil affairs, acted as the interface between NATO and civilian organizations (both local and international) working in Bosnia-Herzegovina. According to the OPLAN, CIMIC units were tasked to publicize their activities in the local and international press. This covers traditional public information activities designed to promote CIMIC operations. Second, the units were tasked to provide information to aid the local populations (civil information). Civil information involved, for example, warning populations about an outbreak of rabies or educating them about the dangers caused by mines. Although U.S. civil affairs units are familiar with these activities, they are not yet part of the developing NATO CIMIC doctrine.…

IFOR QJCIMIC Information Activities

During IFOR operations, civil-military cooperation was principally the responsibility of a 300-personnel unit called the Combined Joint Civil-Military Cooperation (CJCIMIC). The CJCIMIC was both the staff component and advisor to COMIFOR on civil-military issues and a unit whose personnel conducted civil-military activities throughout theater. The CJCIMIC commander designated a lieutenant-colonel (USA) to deal with public and civil information activities. He was tasked to publicize the unit’s activities (in particular with the local press); disseminate all information that might help the local populations; and help in the democratization of the Bosnian media. In addition, the LTC sought to coordinate CJCIMIC information activities with PI and PSYOP. To achieve these goals, CJCIMIC adopted a proactive policy and tried to stimulate media interest in its activities and operations.…

In addition, the CJICIMIC chief of civil information was involved in different programs designed to promote media democratization across Bosnia-Herzegovina. In that regard, CJCIMIC worked closely with the OHR on the Open Broadcast Network (OBN). He also worked closely with the OSCE media development program to run an inter-entity editors group where journalists and editors from all parties (Bosniacs, Bosnian Serbs, and Bosnian Croats) held seminars to discuss free and fair reporting and standards of ethics and professionalism. Four such meetings took place in the course of 1996.

The CJCIMIC information activities encountered numerous obstacles along the road. LTC Brune assessed that civil information campaigns (such as warning about a disease outbreak or informing of disturbance caused by IFOR operations) helped the local communities. On at least several occasions, locals undertook sanitary precautions following CJCIMIC actions. However, the public information campaign quickly faced a major obstacle: “good news doesn’t sell.” As a result, CIMIC operations did not attract major attention from the international press corps (especially in Sarajevo, where there were major policy issues debated)….

Conclusion

Throughout the NATO operations, effectively publicizing CIMIC activities proved a challenge as CIMIC activities did not arouse media interest. In spite of its efforts to publicize its activities, IFOR CJCIMIC found that neither the international nor local media accurately reflected its contributions to rebuilding Bosnia. The situation only got worse with the new rotation of CA unit in December 1996 as the new CIMIC leadership concentrated on command information and did not actively seek to publicize the unit’s operations. At that point, SFOR CIMIC activities were essentially invisible to the international and local publics….

Coordinating Information Activities

Effective communication in Bosnia-Herzegovina required that all purveyors of information disseminate a coherent message in line with what actually occurred on the ground. To ensure message coherence, the commander's information activities within the command had to be closely associated and coordinated with international organizations. However, ensuring coordination was a major challenge. The DPA implementation involved a 36-nation military coalition (IFOR), at least five major organizations (NATO, OHR, UNHCR, OSCE, UNMIBH), and several hundreds of other organizations. Like IFOR/SFOR, most of these organizations had proactive information policies. In addition, three staff components within IFOR/SFOR headquarters (PI, PSYOP, and CIMIC information) worked on information activities. Ensuring harmony and cohesion of message was thus a difficult task.

The Association of PI, PSYOP, and CIMIC Information

Many officers throughout NATO operations in B-H praised the close association between Public Information, Psychological Operations, and CIMIC information. In fact, the unusual aspect most praised was the association between PI and PSYOP. Traditionally, PI and PSYOP activities are separated. The strict separation stems from different missions and philosophies:

- Psychological Operations are an operational tool…designed to influence target audiences' perceptions and shape their behaviors in favor of one's troops and operations.

- Public information…is an operational tool designed to gain and maintain public opinion support for the operation. It is also used as a public diplomacy tool designed to communicate with and pressure adversaries into a friendly course of action. Second, public information results from a basic democratic requirement. It is the means by which a commander reports to the people what their children and tax dollars are used for. It is one means by which a commander is held accountable for his actions by the ultimate source of democratic legitimacy: the public. This democratic requirement entails some obligations, such as truthful and timely reporting within constraint of operational security.

Because of the democratic requirement underlying the public affairs mission, PIOs are generally reluctant to be associated with operations designed to influence attitudes (sometimes through disinformation or deception). For PIOs, being associated with such operations would inevitably damage their credibility with journalists. However, the reality of today's communications renders the strict separation between PSYOP and PI difficult to maintain.…The nature of *Operation Joint Endeavour*, a peace operation, made it possible to closely associate public information and psychological operations. The IFOR PSYOP campaign consisted of convincing the local population (and incidentally the FWF) of the benefits of the Dayton agreement by relying on true arguments.

IFOR/SFOR ran a straightforward PSYOP campaign emphasizing the benefits of democratization and reconstruction and stressing multi-ethnicity. To carry out its campaign, IFOR and SFOR did not resort to deception or disinformation campaigns which might occur in a warfighting environment. Under these circumstances, PSYOP and PI relied on similar arguments and themes. Each staff was entrusted with reaching a specific audience.…PI dealt with local, national, and international journalists. PSYOP carried the IFOR/SFOR message to the local population without the mediation of journalists.…

Conclusion

When implemented, internal and external coordination operated as force multipliers for NATO commanders in Bosnia. During IFOR operations, in particular, internal coordination enabled the commander to use PI and PSYOP effectively to communicate with various audiences. External coordination, especially in the PI field, allowed the international community to develop synergetic information strategies among the main players in DPA implementation. Although coordination proved beneficial, it was difficult to achieve. The IFOR experience showed that external coordination is a give-and-take process which requires compromise, while the SFOR experience showed that successful internal coordination depends on the commander's commitment.

Assessing Information Activities in Bosnia

Operations Joint Endeavour (December 1995-December 1996) and Joint Guard (December 1996 on) revealed the critical nature of information activities in peace operations as the principal means of communication between NATO commanders and various audiences. The overall campaign contributed to mission accomplishment by facilitating communication with the factions and helping maintain public opinion support. However, obstacles and challenges limited the campaign's contribution to mission accomplishment.…

Successes

[NATO's information activites had four areas of notable success: the public information campaign, PI/PSYOP integration within the command group, information as a non-lethal weapon, and coordination with international organizations.]

The Public Information Campaign. The information campaign's primary contribution to mission accomplishment lay in the continued support for or neutrality toward NATO-led operations in the contributing nations. Throughout operations, international and national public opinions showed either support or neutrality toward the mission. No major political controversy emerged at government level (between the executive and legislative bodies, or between the government and political activists) during the accomplishment of EFOR mission. More importantly, a smooth transition from IFOR to an 18 month SFOR mission took place without much difficulties.…

The information campaign was based upon principles that served both the commanders and the international public's needs. By providing complete, timely, and accurate information, the PI0 established its credibility with the international and national media. By establishing credibility with reporters, IFOR/SFOR PI thus reduced the likelihood of unjustified negative stories and gave IFOR/SFOR a better chance to have their side of the story heard. On the media side, reporters publicly expressed their satisfaction with the arrangements made throughout the operations. For most of IFOR/SFOR operations, several internal arrangements adequately supported the requirement for dissemination of complete, timely, and accurate information:

- Allowing a functional chain of information linking PI officers throughout theater proved beneficial. It sped up information flow and allowed PI to provide the media with timely information.
- Appropriate delegation of release of authority to the theater force commander (or whomever he decided to delegate his authority to).
- Close integration with operational staffs and close relationships with commanders.

PI/PSYOP Integration Within the Command Group. The close integration of IFOR PI and PSYOP within the command group also contributed to mission accomplishment. This enabled PI and PSYOP to be more effective tools in the commander's arsenal. Until the transition with LANDCENT (November 1996), PI and PSYOP had close interactions with operational staffs.…Both PI and PSYOP were kept informed of current operations and future plans.…The close relationship eroded after LANDCENT assumed command of the operation. From then on, closeness with commanders receded and integration with other operational staffs loosened.…

Information as a Non-Lethal Weapon. Another important contribution to mission accomplishment was the use of information to enforce the FVVT's compliance with the DPA provisions, deter violence, and resolve crisis. In a peace support operation, where the outside force does not conduct combat operations, the commander has to place a greater reliance on non-lethal weapons. While every unit has some capability in this realm, PI and PSYOP are two critical non lethal weapons. Throughout the operation, commanders made extensive use of public information and PSYOP to help achieve operational goals and relied on information assets (mostly PI and PSYOP) to influence the FWF's behaviors in case of crisis. Adequate information flow and close coordination between staff components allowed the commander to effectively use PI and PSYOP as a non-lethal weapon. It was one of the commander's major tools to communicate intentions, might, and resolve to the local populations and the FWF.

On a routine basis, public information was used to reinforce the appropriateness of IFOR's actions. For example, the MND (SW) commander used his media operations to publicly lay blame on the factions for not fully complying with annex I A of the DPA. In a number of high-profile incidents, IFOR/SFOR and/or the international organizations used public announcements to place pressure on the FWF to enforce compliance with their decisions.

However, information activities are a double-edged sword as they can produce unexpected results. In spring 1996, RS leaders refused to let IFOR troops check an ammunition depot in Han Pijesak. COMEFOR then decided to have his spokesman announce at the daily briefing that IFOR recommended all IOs/NGOs pull out of Republika Srpska, as IFOR was about to use force to support the depot inspection, and they could be at risk for retaliation. After a few days, the RS accepted IFOR's ultimatum and opened the depot for inspection. However, the NGO community was probably more surprised at IFOR's announcement than the RS leaders. Soon after the public announcement, NGO personnel in the RS anxiously called their headquarters back on the Federation side, asking for instructions. Unaware of IFOR's decisions, the I0s were unable to provide any guidance to their operatives in Republika Srpska. This deceptive announcement generated a great deal of mistrust between IFOR and the IO/NGO community.

Coordination with International Organizations. Another important contribution of information activities to mission accomplishment was the fruitful coordination established with international organizations, in particular in the field of public information. Combined activities between IFOR/SFOR, OHR, UNHCR, OSCE, and UNMEBH spokesmen were mutually beneficial at different levels. By accounts of civilian and military participants alike, and in comparison with earlier missions, this was perhaps the most extensive and effective civilian-military cooperation process for PI in a multinational operation. These combined activities symbolized the international community's unity on behalf of peace and reconstruction in B-H. . . .

Although links between the PSYOP and the international organizations were established, they met numerous obstacles. Mutual unfamiliarity between psychological operations and civilian agencies and lack of appropriate structures to communicate requirements complicated the cooperation. Nevertheless, the PSYOP/IO coordination helped familiarize IOs with PSYOP and contributed to the climate of cooperation between civilian and military organizations. PSYOP support to international organizations also enhanced the international organizations' information campaigns. In particular, the PSYOP support enabled the OSCE to run far-reaching campaigns to educate voters on the importance of elections and inform them on the rules and regulations governing the electoral process.…

Limits

The major limit to NATO information activities from December 1995 to fall 1997 lay in its limited effectiveness to offer the local populations a credible alternative view of the international community's efforts to that presented by the factions and to counter local propaganda and disinformation.

The Limited Promotion of NATO's Message. Throughout the operation NATO experienced difficulties in communicating effectively with local audiences. Neither the PIO nor the PSYOP task force were fully adapted to communicate with Bosnian audiences. The original PI planning and initial execution, for example, did not provide for the requirements of local reporters. As PI sought to promote international understanding for the mission, it did not place a high priority on fostering good relations with local journalists. Initially, although NATO PI opportunities were open to local journalists, IFOR made few efforts to accommodate the specific needs of the local press.…IFOR PI developed into a belief that the local media were critical but did not believe they had much impact with local journalists. IFOR, but mostly SFOR, tried to design specific activities targeted at the local media. In particular, SFOR arranged two press conferences a week in RS territory. It also arranged to have a weekly press conference in Serbo-

Croat at the Holiday Inn. However, these efforts were never deemed as important or received significant focus as dealing with international journalists. The CJICTF, on the other hand, was not well-equipped to communicate effectively with a “first-world” audience such as the Bosnian population.…The PSYOP task forces did not have adequate equipment to compete with established media. In particular, the CJICTF did not have a TV capability in a country where an overwhelming majority of people get their news from the local television.

Second, the nature of the IFOR/SFOR message reduced its potential impact. In general, the PSYOP messages were based on general principles…and shied away from difficult issues. For example, the campaign never addressed the fact that the FWF were hindering Dayton Agreement implementation. The campaign also failed to tackle controversial topics such as indicted war criminals out of fear that it could lead to resentment and hostility against NATO troops.…

Overall, several contradictions limited the effectiveness of NATO’s message. NATO could not always follow up a message with relevant action, so there was no positive reinforcement to enhance the credibility of the message. For example, throughout much of 1996, NATO ran a campaign supporting freedom of movement. However, NATO would not and could not guarantee that Bosnians crossing the IEBL into the territory of another ethnic group would be safe. For all practical purposes, the few who undertook such a journey put themselves at risk.…Second, NATO avoided targeting leaders. This approach did not allow condemnation of the political tricks that the factions’ employed to block the peace process. Third, NATO chose not to attack some of the mythologies that block the peace process. For example, NATO has not taken apart the myth that only radical Serbs can protect the Serbs and that the international community is behind some kind of plot to eliminate the Serb people.…Almost no matter the situation, the Bosnian Serb media depicted NATO as some type of evil entity.

Fighting Disinformation. Most of all, neither IFOR/SFOR PI nor the CJICTF was able to fight the factions' disinformation attempts. Confronting disinformation is a difficult problem in the delicate political environment of a peace operation. Through fall 1997, NATO had not adequately answered the challenge of how to respond to dishonest and manipulative factional reporting. In fact, responding to the parties' disinformation seemed to be beyond capabilities and certainly outside perceived mandates.…

Fighting disinformation properly would have required interaction between all staffs in charge of information activities (such as PI and PSYOP) and 02 (intelligence). Such coordination did not seem to take place in Bosnia, at least at SFOR HQ.…

Perhaps because of these weak links, as of spring 1997, no HQ SFOR element tracked disinformation attempts. As far as the author is aware, within the NATO organization, only the SFOR CIO tried to understand factional disinformation attempts. However, he did not have an adequate structure to maintain and analyze a meaningful, comprehensive database. In addition, neither PI nor the CJICTF commanders and staffs campaign thought they should engage in countering disinformation.

A Lack of Vision

In fact, NATO's information strategy was plagued from the start by a lack of vision. With IFOR and SFOR, the NAC did not clarify the mission's end state, but instead relied on two arbitrary, barely believed end dates (12 months in IFOR's case, and 18 months in SFOR's case) to define the mission's final objective.…

This absence of a clear end state hampered both the IFOR and SFOR PSYOP campaigns. Without a clear end state, the PSYOP campaign could not formulate a step-by-step campaign toward a clear objective. During IFOR operations, all information activities were geared toward one goal: NATO is here for 1 year to enforce the cessation of hostilities so the factions can work their differences out. For that year, NATO will use any necessary measure to enforce its mandate, and the factions and civilian organizations have the responsibility to resolve policy issues. This guideline gave the information campaign a direction to work toward. IFOR information campaigns thus mostly focused on force protection issues and NATO might and resolve, and promoted civilian implementation of the DPA. These campaigns successfully conveyed the message that NATO would not tolerate any attack or obstacles to its mission. However, these campaigns did little to help set the conditions for a viable withdrawal of NATO forces.

Right from the start of SFOR's mission, several factors almost immediately prevented the PSYOP campaign from relying on the artificial deadline (June 1998) as its objective. First, several NATO nations hinted that there should be a follow-on force. Second, the Clinton administration ventured to seek support for such an operation and in December 1997 announced an intention to extend U.S. commitment to Bosnia. Finally, NATO's policy toward DPA implementation progressively evolved. In spring 1997, HQ SFOR began exploring a more aggressive approach to DPA implementation and began to work more closely with the international organizations. However, as these changes occurred, no articulated vision had replaced the deadline fantasy and had been articulated to the PSYOP force. As a result, PSYOP personnel did not seem to have a clear understanding of what their mission was and felt they were conducting a wide range of operations without understanding how they contributed to mission accomplishment. Effective PSYOP in Bosnia requires that the CJICTF be given a clear vision of what needs to be achieved.

Learning From Experience? The Transmitters War

Eventually, the information campaign's inadequacies came to light and the international community decided to pay more attention to the issue of media democratization and use of the media to foster the factions' political goals. In May 1997, at the Sintra meeting, the Peace Implementation Council (PIC) tasked the Office of the High Representative with monitoring and sanctioning local media. Although it provided no details on how to do so, the PIC tasked the OHR to enforce democratic and professional media standards. No international institution had had such power in Bosnia until then. Meanwhile, two events gave SFOR a window of opportunity to also strengthen its attitude in that regard.

First, the operation to detain two indicted war criminals in Prijedor (Simo Drljaca and Milan Kovacevic) in early July triggered an angry media campaign by Bosnian Serb media. In particular, SRT portrayed the operation as one more example of the international community’s plot to destroy the Serb people. The campaign heated up when SFOR undertook, in conjunction with the IPTF, searches of RS police stations (in Banja Luka and Brcko) in late summer. SRT drew analogies between the World War II Nazi occupation and the SFOR mission and called for Bosnian Serbs to resist NATO operations.

Second, the power struggle in RS between Momcilo Krajisnik (pro-Karadzic) and RS president Bi1jana Plavsic expanded the international community’s options to deal with the crisis. The power struggle unexpectedly heated up in early summer 1997 when Plavsic decided to dissolve the RS parliament and called for new elections in November 1997. The struggle caused a split within the RS state television, with journalists and editors from the Banja Luka studio deciding to split away from Pale direction after Pale manipulated a broadcast on SFOR searches in police stations.

SFOR and OHR tried to exploit these developments to their advantage. First, SFOR and OHR encouraged SRT Pale to tone down its anti-Dayton, anti-NATO rhetoric with a package of “carrots and sticks.” The OHR negotiated an agreement whereby SRT Pale agreed to stop its anti-NATO campaign and air programs on the DPA sponsored by the international community. In exchange, they would remain open. The sticks came in the form of threats of military action if SRT Pale did not comply. In late September, Belgrade brokered an agreement between Momcilo Krajisnik and Bijlana Plavsic, according to which SRT Pale and SRT Banja Luka would broadcast each others' work on alternate days. For some days, the agreement was honored and both stations toned down their commentaries. However, after SRT Pale heavily edited a tape on the ICTY mission, SFOR seized four transmitters in eastern Bosnia, thus reducing considerably the SRT Pale footprint. At this stage, SRT loyal to Bijlana Plavsic broadcasts across the RS.

The Light at the End of the Tunnel?

Taking down the SDS transmitters and handing them over to Bijlana Plavsic had two benefits. The operation enabled the international community to shut down the most extremist anti-NATO, anti-Dayton propaganda in RS from the largest medium in the country—television. The operation subsequently allowed the international community to increase the visibility of its message in Republika Srpska. But these benefits came at a cost. First, the international community decided to arbitrarily shut down a voice in RS when it had been sponsoring freedom of speech for the past 2 years. It thus found itself in the awkward position of defending curbing the very notion it promoted: freedom of speech and press. Second, there were substantial shortcomings in the planning and execution of these operations which revealed a lack of preparation and vision as to why these operations were taking place. For example, the agreement to broadcast one hour of internationally sponsored program was negotiated without a clear view of how this hour of daily programming would be produced. As a result, SFOR CJICTF was tasked with filling in although it does not have the equipment or resources to produce like a network. In another example, the operation to seize the four transmitters in eastern Bosnia was planned without the PSYOP support. So, after SFOR shut down the transmissions, it had to improvise some actions to explain to the Bosnian Serbs why they were receiving snow on their television sets. A better integration of PSYOP in the planning process would have anticipated this problem and led to a better response.

Finally, taking down SRT Pale transmitters was no panacea. In the new RS media landscape, most broadcast media now back Bijlana Plavsic. Although she has, admittedly, agreed to cooperate with the international community to implement the Dayton Peace Agreement, Plavsic is still a proud representative of Serb nationalism. Her new party, the SNS, is populated with former SDS dignitaries who back the SDS program. Across the country, in spite of the international community's efforts, most local media continue to act as tools of their respective factions. Since early in the war, Bosnia-Herzegovina media were divided along ethnic lines: Bosniacs, Bosnian Serbs, and Bosnian Croats. Throughout the war, local media zealously passed along their faction's propaganda and disinformation. As a result, the factions strictly controlled editorial content. In spite of the international community's efforts, this state of affairs did not stop after Dayton. Local media are still closely tied to the factions and their interests. They spread disinformation as they see fit their factions' political objectives.…

The degree to which the local media are still under the factions' control is worrisome because most Bosnians get their news from and trust most these outlets. According to a poll conducted by the U.S. Information Agency in Bosnia in July 1997, Bosnians tend to rely mostly on “media sources which are closely aligned with parties and/or strongly influenced by regional authorities more than any other.” Bosniacs mostly rely on the pro-government or party-controlled media sources. Bosnian Serbs mostly rely on SRT and Serbian sources from Belgrade (the poll was taken before the break-up of SRT), whereas Bosnian Croats rely mostly on media originating in Zagreb. More importantly, when asked what medium they trust more to report the news accurately, most Bosnian Serbs, Croats, and Bosniacs tend to name the source they use most frequently, e.g., the media controlled by their ethnic group. All the actions taken in late summer and fall 1997, however, only partially addressed the issues hindering an information campaign effective beyond force protection issues….

Identifying Lessons from the Bosnia Experience

…the following paragraphs highlight some of the key lessons identified in the experience of information activities during the first 20 months of NATO operations in Bosnia-Herzegovina.

Clearly Articulate PI Principles and Guidelines

Clarity of guidance is a principle that all military commanders understand. General Joulwan and Admiral Smith provided clear and straightforward guidance for their PI officers to follow. These principles (complete, accurate, and timely reporting) lay at the core of PI activities throughout Operations Joint

Endeavour and Joint Guard. The success of these principles highlights two points. Just as elsewhere in the operational planning, a commander must pay attention to what he expects from his PI officers and must provide guidance so that they can achieve what he expects. In addition, these specific principles well served the military force and NATO overall through the period analyzed.…

Adapt PI to the Speed of Media Reporting

Technological advances have combined with concepts of media professionalism to greatly diminish the time it takes for something to happen and for the world to have access to reporting (accurate or otherwise) about those events.…For the PI (and rest of the force) to effectively deal with the reality of today's (and tomorrow's) journalism, several steps seem key:

- Establish a chain of information: The military process of information is often too slow to keep up with the fast speed of media reporting.…
- Delegate release authority downward: A military commander cannot have an effective public information campaign if he must seek national approval before opening his mouth. The best approach is to establish the parameters within which the commander is allowed to speak.…

Strengthen Psychological Operations

Psychological operations contribute to OOTW in several ways. By communicating the appropriate message, a PSYOP campaign can enhance force protection and help convince the local population to support the operation's final objective. To effectively contribute to mission accomplishment requires that several conditions be met:

- Tackle difficult and controversial issues:…PSYOP campaigns should not shy away from tackling difficult issues…
- Undermine adverse propaganda:…it is likely that other parties will be using media and other propaganda tools to spread a message counter to the international community's interests. The PSYOP force should provide the key military element to deal with such elements: tracking, analyzing, and countering these propaganda efforts.
- Back messages with action: Messages should be tied to concrete action. Constantly reemphasizing messages that do not comport with reality (such as talking of freedom of movement in Bosnia-Herzegovina when every local was nervous about traveling into another ethnic group's territory) will undercut credibility…

Adapt to Local Audiences

In OOTW, winning the hearts and minds of the local population is important. As with any other type of operation, a commander's goal is to avoid local population interference with operations. But in a peace operation where the use of force is limited, persuading the locals to support the operation and potentially using it to apply pressure on uncooperative local authorities will enhance mission accomplishment. To improve the odds that the local population will accept the message, the campaign must be adapted to the local audiences. The following are three steps to achieve this:

- Tailor the message appropriately. The PSYOP operation must tailor its message to local audiences' knowledge and culture. In addition, dissemination needs to fit the locals' media consumption habits.
- PI should not neglect local media. PI officers typically focus on international and national publics.…This focus, however, should not be at the expense of local journalists, especially when they are the primary source of information for the local population…
- Use the force to communicate with locals. To a large extent, any soldier's interaction with the locals can be used to foster the commander's goals. Force posture sends a message. Daily interactions between the soldiers and the local population can be used to disseminate further the commander's message.

Associate PI, PSYOP, and Civil Information

To increase their effectiveness, closely associate information activities. The close association between PI, PSYOP, and civil information should aim at coordinating and synchronizing the messages so they reinforce each other. If the PSYOP campaign is engaged in grey or black propaganda, however, this close association could become inappropriate.

Integrate PI/PSYOP with Command Group and Establish Close Relations with Commander

The PIO and PSYOP commander cannot be fully effective without a close relationship with the commanding general. From the earliest stages, these officers must be strongly established as key actors in the command group. Commanders should assure strong ties with these key non-lethal weapons. This could involve, for example, holding daily (small) infon-nation meetings as well as direct access to the commander.

Coordinate Internally

Fully effective information activities are tied into the operations. Close integration with other operational staffs (in particular the Y shop) allows information activities to be used effectively to prepare for and better respond to contingencies and to refocus the effort when necessary. To achieve such level of integration requires internal coordination whereby PI, PSYOP, and civil information hold regular meetings with operational staffs to receive their inputs on the information campaign and channel feedback into the headquarters.…

Coordinate Externally

The military is not the only actor in OOTW. In peace operations, the military will work alongside civilian international organizations such as the United Nations, the High Commissioner for Refugees, and the World Bank. Coordinating, cooperating, and working with these organizations will enhance overall mission effectiveness and speed mission achievement.

Information activities is one of the areas which will gain with such cooperation.…

Clearly Articulate an End State

Like every other element of an operation, information activities' effectiveness will be hampered (if not crippled) if the political leadership cannot (and does not) clearly articulate a concept for the mission's end state. The absence of a clear end state makes it more difficult to develop a successful information strategy. To develop a convincing and credible position, the PSYOP and PI need to have a clear objective in mind, so they can work backwards to develop the necessary steps leading to the final objective. A viable end state is fundamental both as the objective which helps to define a strategy and as a measure of success or failure for the mission. Without an idea of where they are supposed to be heading, no element of information activities will be fully effective in their endeavours.

These lessons do not necessarily constitute a blueprint for success. However, adopting the lessons identified from the Bosnia experience (both the positive and negative experiences) will make future U.S. and multinational peace operations more effective and more likely to achieve mission objectives.

CHAPTER 21

KOSOVO AND THE CURRENT MYTH OF INFORMATION SUPERIORITY

By
Timothy L. Thomas

The Pentagon's March 1999 brochure on information operations begins with a few words from the Chairman of the Joint Chiefs of Staff, General Henry H. Shelton. He notes that "information operations and information superiority are at the core of military innovation and our vision for the future of joint warfare.…The capability to penetrate, manipulate, and deny an adversary's battlespace awareness is of utmost importance."[1] The Pentagon's brochure adds that "the chief concern of information superiority is the human user of information. Without knowing when, where, why, with what, and how to act, warfighters cannot perform mission-essential tasks efficiently and effectively."[2]

Kosovo, unfortunately, exposed problems with this concept. First, in spite of NATO's near total information superiority, its battlespace awareness was manipulated by the Serbian armed forces more often than expected. When human and software interpreters of intelligence information were fooled, it resulted in munitions wasted on fake or incorrect targets and in bad assessments of the actual situation on the ground.

It also affected both mission essential tasks and battle damage assessments. In the latter case, it meant different estimates by NATO and Pentagon officials of the number of armored vehicles destroyed.

Second, testimony indicates that both NATO planners and the human users of information were not adequately prepared to conduct information operations. For example, in their lessons-learned testimony before the Senate Armed Services Committee on 14 October 1999, Secretary of Defense William Cohen and General Shelton noted that “the pool of personnel available to perform certain key functions, such as language translation, targeting, and intelligence analysis, was limited” and that “the conduct of an integrated information operations campaign was delayed by the lack of both advance planning and strategic guidance defining key objectives.”[3] But planning had started in earnest in the summer of 1998, Cohen and Shelton testified, some nine months before the start of the conflict on 24 March 1999. Did initial planning not include information operations?

Finally, General Wesley K. Clark, Supreme Allied Commander Europe, reportedly stunned a recent session of the Senate Armed Services Committee when he called for a complete rethink of Western strategy and questioned the need for the aerial assault on Serbia. General Clark noted that NATO could have used legal means to block the Danube and the Adriatic ports, and could have used “methods to isolate Milosevic and his political parties electronically.”[4] If implemented and augmented with other measures, Clark added, the military instrument might have never been used.[5] These and other issues demonstrate that, for the present anyway, information superiority is a goal to be achieved and not a given that U.S. forces can assume as their birth right.

This article will look at the conflict between NATO and Yugoslavia not from the standpoint of the intent or success of the air campaign (although these issues will be touched upon) but rather through the prism of information superiority. Information superiority allowed NATO to know almost everything about the battlefield, but NATO analysts didn't always understand everything they thought they knew.

What Is Information Superiority?

Information superiority, the cornerstone of Force XXI, is a capability (not a proven condition) that the U.S. armed forces are trying to develop. Once the concept becomes robust it will help to reduce uncertainty, provide a more complete intelligence picture of the battlefield, and assist precision-guided missiles in obtaining and destroying targets. Much of this capability was on display in the recent conflict in Kosovo.

Information superiority is defined by *U.S. Joint Publication 3-13* as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[6] According to this definition, NATO's forces entered the Kosovo conflict with near total information superiority. It appeared that NATO was able to collect, process, and disseminate military information at will while denying the Serbs the same capability. However, NATO forces did encounter intelligence and information problems, including instances of the Serbs using nontechnical methods to manipulate NATO analysts' perceptions, resulting in misinterpreted information. *Joint Publication 2-01* warns about this phenomenon in a discussion of the "intelligence cycle." The publication notes, "Time constraints and the demands of modern battle tend to make the processing and production phases indistinguishable."[7] This in turn limits "evaluating, analyzing, and interpreting information from single or multiple sources into a finished intelligence product."[8]

In addition, Serbian civilian and military personnel were able to use civilian telephone and radio links to pass military information. Such nontechnical offsets either thwarted information collection or corrupted NATO information superiority. That is, the human link in the NATO analytic process was less successful in interpreting information, reducing uncertainty, and providing a clear intelligence picture of the battlefield than expected. For example:

- Some 6 months after the conflict, NATO and the Pentagon still did not know how many tanks and armored personnel carriers they destroyed, in spite of supposed total information superiority during the conflict, the ability to monitor Serb forces leaving the area after the conflict, and the presence of their own people on the ground to inspect targets that were hit.

- NATO pilots were forced to drop millions of dollars of ordnance in the Adriatic and on open countryside because they could not find their targets or engage them properly due to bad weather and the aerial rules of engagement (ROE) imposed by politicians. (The planes could not land with the unexpended ordnance on board.) Since the ROE were imposed by politicians, this means that politicians affected information superiority, too.

- NATO after-action reports stress that Milosevic may have intercepted NATO communications and warned targets that they were about to be hit. The testimony of Secretary Cohen and General Shelton supports this thesis. They indicated that NATO lacked interoperable secure communications, forcing reliance on nonsecure methods that compromised operational security.[9] This speaks poorly about the progress of communications technology, compatibility, and information superiority in NATO after 50 years of practice (and in this case with no enemy radio-electronic opposition of any consequence).

- NATO had almost perfect intelligence about the intentions, goals, and attitudes of President Milosevic through a multitude of personal discussions with him over the previous 4 years by representatives from scores of nations (and possibly from communications intercepts), yet could not get him to the negotiating table, foresee his ruthless ethnic cleansing campaign in time to stop him, or predict his asymmetric responses to NATO technological and bombing prowess.

Further, NATO did not process information quickly enough to enable aircraft to strike mobile targets. This was because of the reaction time required to pass data from EC-130 (airborne command, control, and communications) aircraft to NATO’s Combined Air Operations Center at Vicenze, Italy, and then on to strike assets. Total information superiority did not prevent the most technologically advanced air armada in the world from mistakenly striking trains and convoys, schools and hospitals, and Bulgaria with missiles. Yes Bulgaria, the wrong country, although that incident was the result of a weapon system malfunction, not an error in the application of information.

Two important qualifiers are missing, but implied, in the *Joint Publication 3-13* definition of information superiority: “accurate” and “timely.” Information superiority requires the “accurate and timely” collection, processing, and dissemination of information. Battle damage assessments on armored vehicles indicate that the accuracy of hits on mobile targets, for example, was much lower than originally stated. Such inaccurate information can lead to wrong conclusions and assumptions. For example, NATO claims that 99.6 percent of the bombs dropped hit the intended target are difficult to fathom.[10] Undoubtedly the percentage differed for stationary and for mobile targets. And does this figure reflect that some bombs hit fake targets, and that many bombs had to be jettisoned into the Adriatic due to bad weather or because a target had moved? Only after illuminating the data with such criteria can a real assessment of accuracy be made. A lower figure—perhaps 80 percent—might be a more realistic assessment but still a perfectly acceptable measure of success.

Strikes on fake targets indicate that the Serbs let NATO daytime reconnaissance flights see real targets and then replaced them at night, or that U.S. target analysts misinterpreted the information furnished them. Processing information is one thing, interpreting it is an art. Serbian civil and military officials improvised and developed low-tech offsets that limited the effectiveness of NATO’s information superiority and misled NATO collection assets. Put another way, they fooled our information interpreters. Their offsets included deception, disinformation, camouflage, the clever use of radar, spies within NATO, helicopter movements NATO couldn't detect, and the exploitation of NATO's operational templating of information-dominance activities (e.g., satellites, reconnaissance flights). As Lieutenant General Michael C., NATO's air operations chief, noted, "NATO placed its own air crews at increased risk by taking certain steps to reduce civilian casualties, such as bombing bridges only on week nights between 10 p.m. and 4 a.m.—a regular schedule that made NATO planes more vulnerable to antiaircraft fire."[11]

Additionally, Serbia exploited the strict rules of engagement to protect or move certain target sets. This further limited the effectiveness of NATO's information technology. For example, NATO aerial ROE stated that pilots could fire only on visual recognition, diminishing the value of targets obtained by other methods. Finally, political statements that no ground campaign was planned allowed the Serbs to hang on longer against an opponent with total information superiority and attempt to exploit any cracks in NATO's solidarity. One can conclude there are ways to manipulate total information superiority.

Digital interpreters of data differ from the old intelligence analysts who worked with photos and captured documents to interpret data. The former must be aware of and study nontechnical offsets in addition to technologically produced intelligence, and constantly review the methods they use to interpret data. There is much to learn from Kosovo about the current myth of information superiority, particularly that simple human innovations can severely degrade digital dominance, and that human interpretation of data is a science worth reinvigorating.

NATO's Information Superiority

The conditions were right for NATO to achieve total information superiority. There was virtually no air force flying against NATO's 37,000 sorties (Serbs flew only some 10 air intercept or fast-mover missions). NATO faced antiquated, minimal enemy air defense artillery assets developed in the 1950s through the 1980s that couldn't reach above 15,000 feet. No real counter-radar challenge was offered since the air defense assets that could reach higher were not turned on. NATO possessed the ability to pinpoint targets using Predator and Hunter unmanned drone aircraft as well as satellite and JSTARS intelligence links, yet made mistakes. There was a huge assortment of intelligence products on hand concerning Belgrade and Serbia based on several recent field exercises. There were elements on the ground to assist in the effort, including personnel from the Kosovo Liberation Army. There was no Serb jamming of communication or radar assets. Total NATO information superiority was at hand. Yet errors were made in the selection of buildings to be hit, most notably the Chinese embassy.

In spite of this superiority, a ground operation was almost launched. *The Washington Post* described top-secret talks among NATO countries' defense ministers at the end of May to plan a ground invasion. That is, flying with impunity, grounded only by bad weather, NATO mounted a 78-day air campaign (Desert Storm's lasted 43 days) and this still wasn't enough. NATO was forced to stand down a last-minute scramble to mount a ground campaign. (Planning for such an operation had taken place much earlier. The reference here is to moving forces into position to cross the Kosovo border in an underdeveloped theater, where the force in place was attending to the needs of thousands of refugees, and to conduct operations before winter.) It took a combination of an underrated assist from President Martti Ahtisaari of Finland and former Prime Minister Victor Chernomyrdin of Russia, the threat of a ground operation, and the air campaign to actually achieve a negotiated settlement and later a capitulation to stop the air war. General Wesley Clark, Supreme Allied Commander Europe, noted that Milosevic probably caved in simply because he ran out of options.[12]

The air campaign, however, was the signal event of NATO's strategy. The pilots and support personnel should rightly receive nearly all the credit for making Milosevic blink. On the other hand, what did the air campaign eventually achieve? Achievements should be viewed in accordance with both political and military measures. A logical political expectation would be that the Milosevic government would sign Rambouillet Two or some other agreement less acceptable to Yugoslavia, since Serbian reluctance to sign this document was the motivation for going to war. But Rambouillet Two was not signed and the Belgrade Agreement that was signed delivered something far less. That is, the prosecution of the air campaign did not lead to NATO getting what it originally wanted. The question must be asked, was the air campaign unsuccessful in the political respect because NATO's initial demands were too high?

On the other hand, military planners state that the intent of the air campaign was to negate the effective use of Yugoslav forces in Kosovo and ultimately eject those forces from Kosovo. This was accomplished by the use of air power, and no one can dispute this. Simultaneously, however, Yugoslav paramilitaries and police began their ethnic cleansing operation which the air campaign could not target. The air campaign was unable to target individual policemen or other ethnic cleansers unleashed by Milosevic. Was a ground operation needed to prevent the ethnic cleansing? Did the successes of the international negotiators and the threatened ground force intervention at the time that Milosevic threw in the towel mean that the air campaign "was successful because it failed"?[13] That is, the air campaign was not able to deliver an end game by itself without the combined threats of a ground attack and the negotiating prowess of the Russian and Finnish participants.

There is much to ponder and learn from the conflict in Yugoslavia. However, Kosovo should not be considered a typical future conflict on which to base subsequent contingencies. NATO and U.S. leaders cannot plan on always flying without opposition (or having unimpeded communications). Kosovo and, to a certain extent, Desert Storm were aberrations in that regard. Another danger is the tendency of some officials to spout euphoria about the "matchless" NATO force and its unrivaled capabilities. "Matchless" when pitted against what—the air defense forces of Iraq and Yugoslavia? Neither NATO nor the United States has fought a modern, up-to-date power. Finally, another lesson to be learned is that even without information superiority, a thinking opponent can take actions that must be countered. Clausewitz noted this lesson in his own century.

Battle Damage Assessment: What Do We Believe?

One of the major indicators of the myth of information superiority is the ongoing examination of battle damage assessment. This is particularly the case with official figures offered by the NATO Supreme Allied Commander and the Department of Defense versus those of foreign defense departments and independent reporters.

The Views of General Wesley Clark, Supreme Allied Commander, NATO

It is important to note that this analysis is simply an attempt to express the concern generated by sets of figures that do not correspond to one another. It is not an attempt to cast doubt on General Wesley Clark, who has received far less credit than he deserves for keeping the alliance together during the conflict. General Clark does not count tanks; he relies on figures provided by others. It is fair to examine the figures he is being provided, however, and to consider how he chose to use them.

On 12 July, 1 month after the end of the bombing, the Navy Times discussed General Clark’s testimony before the Senate Armed Services Committee. Relying on information provided by his staff, Clark stated that reports about NATO warplanes striking decoys and failing to destroy tanks and personnel carriers was a concerted disinformation campaign. Rather, he chose to underscore the virtual invulnerability of NATO aircraft and the fact that Kosovo set a new standard for warfare. He did not mention that there was no air force flying against NATO, nor that the 15,000-foot limitation was set to ensure there would be no damage to NATO's "virtually invulnerable" fleet. Battle damage assessment, according to Clark, included the destruction of 110 Serb tanks, 210 armored personnel carriers, and 449 guns and mortars. He also noted that NATO was aware the Serbs were using decoys and were able to recognize them. Department of Defense estimates of battle damage were slightly higher than Clark's estimates (120 tanks, 220 armored personnel carriers, and 450 artillery pieces).[14]

Clark later offered a reason why the battle damage may not have been as high as initially expected—there was a spy within NATO giving targets away to Belgrade. *The Pacific Stars and Stripes* quotes Clark on 13 August as saying the leak "was as clear as the nose on your face."[15] That is certainly one form of asymmetric offset to information superiority, and again it involves the human dimension. Even with complete information superiority, one can't destroy the target if the enemy knows an attack is coming and simply moves it or replaces it with a dummy target. NATO officials were reportedly tipped off that a spy might be among them by the fact that certain targets appeared to be vacated after appearing on target lists but before NATO planes attacked.

In September, a Pentagon review of the war was delayed by one month in order to fill in gaps in the number of armored vehicles and artillery batteries actually destroyed. One report noted that General Clark told a Pentagon officer that analysts verified only some 70 percent of the reported hits. Clark then ordered the U.S. European Command to prepare a new estimate as well.[16] In a later report, Clark lowered his battle damage assessment, noting that in all likelihood only 93 tanks and 153 armored personnel carriers were destroyed.[17] The difference—17 tanks and 57 armored personnel carriers—is close to two reinforced infantry battalions. That obviously would be an extremely significant difference to a ground commander preparing for an attack. Accurate damage assessments are crucial to a ground commander's maneuver requirements.

Even with total information superiority, it was not possible to verify battle damage with any accuracy some 2 months after the conflict ended, despite having NATO forces on the ground and overhead coverage of departing Serb vehicles. Since DoD and NATO still have not produced a compatible set of figures to this day, there clearly is a faulty methodology or other problem here as well. All of these hits were cockpit recorded and many were shown on TV. There should be near compatibility between NATO and Pentagon findings in the age of information superiority.

The British Press and Other Reporters on Battle Damage Assessment

Independent accounts from reporters covering the battle for Kosovo offered an entirely different set of battle damage statistics from those offered by either General Clark or the Pentagon. Their perspective is interesting for it is offered from firsthand, on-the-ground analysis, just like the latter NATO and Pentagon estimates.

The first newspaper reports on battle damage appeared at the end of June. Indications were that only 13 Serb tanks and fewer than 100 armored personnel carriers had been destroyed. Reporters noted the ruins of many different types of decoys hit by NATO forces (e.g., rusted tanks with broken parts, wood or canvas mock-ups). Carlotta Gall of *The New York Times*, a veteran war correspondent from the first Russian war in Chechnya, saw little damage. *Newsweek* reporter Mark Dennis found only one destroyed tank after driving around Kosovo for 10 days. Did the Serbs manage to extricate all of their destroyed vehicles during their publicly filmed withdrawal, did they hide them, or did they really experience much less damage than NATO sources declared?

In late July, *Aviation Week and Space Technology* reported that NATO had dropped 3,000 precision-guided weapons that resulted in 500 hits on decoys, but destroyed only 50 Yugoslav tanks. Deputy Defense Secretary John Hamre also reported that all 30 (other sources use the figure 20) incidents of collateral damage would be studied (the trains, convoys, schools, hospitals, and Bulgarian strikes).[18] What types of bombs actually hit the decoys is known only by Pentagon insiders, so they are the only ones capable of calculating the amount of money wasted on these targets. This is an important issue, however, because early in the war NATO and U.S. stocks of precision weaponry ran very low, a fact that undoubtedly was noted and highlighted by other nations with hostile intent toward the alliance. They received a yardstick measurement of how long an air campaign can proceed using certain types of high-tech armaments against specific targets before stocks run low.

U.S. News and World Report, in its 20 September 1999 edition, stated that a NATO team visited 900 "aim points" targeted by NATO in Kosovo and found only 26 tank and similar-looking self-propelled artillery carcasses. This would again throw NATO's revised number of 93 tanks out the window. However, how many tank carcasses were in Serbia, where the NATO team did not visit, is not known, making this figure less provocative and contradictory than it originally appears. The article also reported increased friction between General Clark and his NATO air operations chief, Lieutenant General Michael Short, over target selection and strategy (mobile targets such as tanks versus infrastructure, respectively). The article concluded that it was not air power but Russia's withdrawal of support for Serbia that probably brought an end to the air war in Kosovo. The article noted that in future conflicts, the most merciful way to end them may be to conduct them swiftly and violently instead of by the trial-and-error phased approach used in Kosovo.[19]

Finally, several British officers, both retired and serving, also noted that damage was much less than originally stated. One newspaper report, citing British Ministry of Defense sources, stated that the damage done to tanks was perhaps even less than the lowest quoted figure of 13 tank kills.[20] But the most damning comment could prove to be from an *International Herald Tribune* article on 1 October. Written by Frederick Bonnart, the editorial director of the independent but highly authoritative *NATO's Nations*, the article discusses how NATO "propaganda" was used against the West. He notes:

> *In democracies, it is the duty of the public services to present the truth even in wartime, and particularly when they are in sole control of the information. If it is deliberately designed*

> *to engender fear and hate, then the correct term is propaganda.*[21]

In particular, Bonnart believes the armored vehicle totals did not properly represent the vehicles actually destroyed, and that NATO deliberately used the West's reputation for truth and fairness to carry out a highly charged information policy against the Serbs. This made NATO's information policy rife with propaganda, Bonnart contends, and he points out that recommendations are being prepared to create a future NATO crisis information organization to keep this from happening again.[22] When did we ever think that a NATO-oriented publication's editor would be publicly accusing SACEUR's organization of propaganda and disinformation?

Assessing the Results of Information Superiority

One danger of the air campaign over Yugoslavia is overestimating NATO and U.S. capabilities. All of the systems did not function all of the time with perfection. For example, some of the high-tech systems were unable to operate under poor weather conditions, as underscored in the daily Pentagon briefings during the campaign. Certainly it was an exaggeration to say:

> *A vast number of intelligence, surveillance, and reconnaissance systems allowed for the rapid collection and collating into a single system the vital battlefield intelligence that we sent to our shooters. Taken together, all these innovations allowed our pilots to hit any target, any time, day or night, in any weather, accurate to within a few feet.*[23]

Secretary of Defense William Cohen, in a November speech in California, listed several extremely important qualifiers regarding capabilities. He noted that even the most advanced technologies have limits and that a precision-guided weapon can only hit the coordinates it is given. Moreover, "our vast intelligence system can create such a haystack of data that finding the one needle that will pinpoint a target in the right time frame is difficult, indeed."[24]

Hitting the right target on time requires sorting out the right coordinates from a pile of information (interpreted correctly) at the right time, a degree of data management that is difficult to achieve. Yet that, most believe, is just what information superiority was designed to do. It is clear from the Secretary's comments that much work remains. His "technologies have limits" qualifier requires our attention. This is perhaps a recognition that our systems still cannot, as evidenced by Kosovo, determine if a target is a fake, and this in an environment where we were not confronted by opposing information technology systems to disrupt friendly systems. As a result, NATO and the United States lost untold resources each time we expended ordinance on impostor targets.

Does a count of destroyed tanks matter? When counts are off by such a margin, they do. A comparison of these figures causes the average American to shake his head in confusion and frustration. Worse yet, these figures affect American lives. The interpretation of data by analysts at the lowest level also directly affects the credibility of our leaders and commanders who must stand before service members and the American public to relate the data. The problem is analogous to that encountered with counting SCUD missiles during Desert Storm. Coalition assets often hit gas or trailer trucks instead of missile launch vehicles for the same reasons. We haven't corrected this problem, and maybe it is simply beyond our ability to do so with current technologies. But we must face up to our shortcomings if we want to do better. Concern over battle damage assessment is not analogous to the Vietnam era's "body count" fixation, as some try to imply. Rather, the battle damage assessment debate is over just how much of our battlespace awareness was manipulated, and that does matter.

Another problem with disputes over battle damage assessment in Kosovo is that focusing on that aspect loses sight of the actual war that Milosevic fought (and not the template war that NATO assumed he would fight). Milosevic's real war was the ethnic cleansing offensive against the Albanian civilian population of Kosovo. Milosevic had two objectives. The first one was immediate, to rob the Kosovo Liberation Army (KLA) of its medium of support. The second objective was the campaign against NATO's center of gravity, its political stability. Milosevic confronted the United States and its allies with the grave risk of expanding instability throughout the "target" countries of Albania and Macedonia, and extending into the entire Balkan region. His instrument in this campaign was primarily paramilitary and police formations which left little information signature. This made targeting armored vehicles and artillery systems largely irrelevant to countering Milosevic's offensive. Additionally, targeting the Yugoslav infrastructure offered only protracted operations with significant economic damage to all of southern Europe, whereas the refugee problem was immediate and catastrophic. Milosevic proved he was a master at playing chess while his NATO counterparts played poker.[25] This made General Clark and General Short's arguments over targeting at best tangential to the war Milosevic was imposing on his opponent.

Asymmetric Offsets to Information Superiority

Admiral James Ellis, Commander-in-Chief of NATO's Allied Forces Southern Europe, noted in an interview on Kosovo in early September 1999 that too much information has the potential to reduce a military leader's awareness of an unfolding situation. Too much data leads to sensory overload: "Information saturation is additive to the 'fog of war'…uncontrolled, it will control you and your staffs and lengthen your decision-cycle times."[26] Admiral Ellis extended this problem to video teleconferencing as well, since it can become "a voracious consumer of leadership and key staff working hours."[27] This is probably the most interesting and underrated lesson learned of the entire war, that information superiority overload can actually hurt mission performance. Whether this fact influenced the tank count is unknown. Secretary Cohen also mentioned this problem in his speech in California. The point to make is that perhaps this flood of information in its own way the human interpreter's evaluation of the situation on the ground. Technical systems provided "proof" that a tank had been destroyed, when in fact the target hit wasn't a tank.

Admiral Ellis also recounted some of the asymmetric Serbian responses during the conflict, sighting the following: sporadic use of air defense assets; deceptive media campaigns; deliberately increasing the risk to NATO pilots of collateral damage; and developing political cleavages between NATO allies. To prevent its air defense assets from being neutralized, the Serbian armed forces turned their assets on only as needed. They therefore presented a "constant but dormant" threat. This resulted in NATO using its most strained assets (e.g., JSTARS, AWACS) to conduct additional searches for air defense assets and forced NATO aircraft to fly above 15,000 feet, making it difficult for them to hit their targets. Ellis noted that NATO achieved little damage to the Serbian integrated air defense system.[28]

Admiral Ellis also spoke about not being able to counter Milosevic's state-controlled media and his attempts to gain international sympathy. As Milosevic's forces killed hundreds of people, NATO was always responding to its collateral damage problem. This is another lesson that must be addressed, how to prevent the press from becoming an asymmetric asset for the enemy.

Regarding the media, the U.S. military's airborne psychological warfare machine, "Commando Solo," was unable to affect the Serb state media. Its use was hampered by the unknown air defense threat in the area. NATO officials were unwilling to risk flying the plane over Belgrade in fear that Milosevic would trade an air defense site in exchange for shooting down the slow-moving platform. As a result, Commando Solo flew far away from the Serb capital and was unable to affect TV coverage. One report during the bombing campaign asserted that NATO had proposed a moratorium on the bombing if Milosevic would just give NATO 3 hours of air time on TV and radio each evening. This indicates how unsuccessful the psychological warfare plan had become. All the while Milosevic maintained information superiority over his own people.

The expectation that the air campaign would last only a short time also was a detriment to the NATO psychological operations effort, since those assets were not included in the initial plans. It took two weeks to start delivering products and some 30 days to develop a campaign plan. Serbia started its psychological operations campaign days earlier and won the early initiative. The Serbs were initially successful on two fronts. First, they instituted the "target" campaign among their own people, in which citizens adorned themselves with bulls-eye targets, as if daring NATO to strike them personally. This idea greatly enhanced Serb morale and resistance at the start of the conflict. Second, they used the Internet to spread various campaign themes and claims, an effort the former U.S. Information Agency (USIA) worked hard to control. One USIA analyst believes the conflict was the first Internet war, with both sides using the electronic medium to fight one another in a war of words and logic. But the point to again be made is that at the start of the conflict Serbia maintained information superiority over the minds of its citizens.

Another asymmetric offset, one not noted by Admiral Ellis, was the ability of Milosevic's air defense personnel to template U.S. and NATO air operations based on their performance during the Gulf War and in Bosnia. Knowing when reconnaissance flights would be conducted, or when satellites would fly overhead, the Serb military would preposition armored vehicles to be picked up as targets. Then the Serbs would move the actual targets; in some instances they put in the target's place an old tractor with a telephone pole attached to make it look like a tank from 15,000 feet. At night it was difficult to tell the difference. And, it must be remembered, NATO pilots still had to contend with the possibility that air defense assets could be turned on and fired at a moment's notice, reducing their target focus.

In hindsight, NATO did not handle the political side of information superiority well either. The alliance had the combined assets and knowledge of its 19 nations to draw on in composing a psychological and negotiating profile of President Milosevic. From this background, political analysts around the world should have able to draw a reliable profile of Milosevic's intentions, goals, and desires. In addition, NATO had the negotiating edge at Rambouillet. Some believe, however, that a mistake was made in the form of an ultimatum to Milosevic that ended the talks. Many diplomats apparently expected the ultimatum to result in a quick capitulation or a Milosevic retreat.[29] That did not happen. Instead, look at the results: at Rambouillet One, Albanian moderates signed the agreement; at Rambouillet Two, the KLA signed in the expectation that elections for Kosovo would be held in three years, and that NATO transit in Serbia would be allowed; and at the final moment when the Belgrade Agreement was signed, neither of those two conditions survived.

One hopes that State Department analysts are studying in depth these negotiating shortcomings and the inability to persuade Milosevic, just as the military should be studying the shortcomings in its information superiority approach. For example, did diplomats and military representatives alike make the wrong assessment of the projected length of this conflict based on Milosevic’s behavior following NATO’s air campaign in August 1995? The 1995 concessions were likely the result of the combination of the air campaign and the simultaneous ground force offensive that was under way in Croatia, not just the bombing campaign alone. Did planners overlook this? Undoubtedly, Milosevic was to some extent irrational, but we also knew him well and should have been able to foresee his responses with some degree of certainty based on previous conversations and actions.

Technological and Political Fixes

Of course attempts are being made to correct some of the technological problems encountered during the conflict in Kosovo. NATO technical weaknesses included an inability to identify moving targets and to find armored or other equipment that was well camouflaged. The director of the Defense Advanced Research Projects Agency (DARPA), Frank Fernandez, is trying to solve both of these problems. He noted, “You had to put a human eyeball on [a] target before you could give the command to shoot because we don’t trust our identification systems.”[30] Again, the human dimension is stressed. Initial areas of intensified DARPA research include:

- Improving a sensor’s ability to identify targets and see through camouflage.

- Reducing the size of space radars and their antennas to more accurately sense moving targets.

- Finding better methods to combine and pass target data through networks to aircraft or weapons.

- Developing techniques to find underground facilities and see what is happening inside.
- Establishing tactics for accurately striking moving targets in bad weather.[31]

The efforts to identify moving targets are focused on multi-, hyper-, and ultra-spectral (optical) sensors that take electromagnetic spectrum slices to identify targets. Technologies to uncover camouflaged equipment will take advantage of operational sequencing of various types of targets to uncover them, as well as low-frequency radars and computer programs designed to see through foliage. Finally, Fernandez noted that future attacks will be based on a piloted vehicle operating in tandem with two or three pilotless vehicles: "That's what we learned in Kosovo—to strike these targets that are hidden took two people, one to fly and release the weapon and another to look for and designate the targets."[32] Fernandez's desire to have a human assist pilotless vehicles is important because it indicates that DARPA may not fall prey to an American tradition—trying to just find technological answers to problems.

It also will be interesting to watch the explanation of political learned over the next few months. For example, there should be a serious effort at the State Department and in the National Security Council to right some apparent wrongs in our decisionmaking process. Wouldn't it be wise to study why we failed to develop a campaign plan beyond the first 5 days? And shouldn't we study why we put our operational art in the hands of politicians who tried to dictate the pace, scope, and rules of engagement, and perhaps even the target selection process? Wouldn't it be advantageous to find new ways to persuade the Milosevics of the world to negotiate, allowing NATO and the United States to withhold the use of their war machine in the first place and thus not having to deal with the technological problem sets of such a conflict? Wouldn't this be better than simply developing new technological solutions?

Conclusion

Why is information superiority a dangerous myth? Primarily because we don't interpret what we collect as well as we might. It is not that we are doing poorly, just that we aren't doing as well as we think we are. Consider, for example, the shortcomings sighted above of NATO's use of total information superiority:

- Total information superiority did not allow us to achieve a political or diplomatic victory. Like Saddam Hussein, Milosevic is still in power, and the Belgrade Agreement was a far cry from what was sought at Rambouillet.

- Total information superiority did not enable NATO to locate the Serbian armed forces' center of gravity, the police, and paramilitaries doing the killing.

- Total information superiority did not counter rumor nor prejudiced reporting. For example, to cite an instance not covered in this analysis, information superiority did not allow NATO to know, even approximately, how many Kosovo civilians were killed before the bombing started. Instead of 100,000 Kosovo victims, as rumors suggested, 10,000 now appears to be closer to the truth. Would NATO have gone to war over 10,000 people? To date, only some 2,500 bodies have been discovered.

- Total information superiority was affected by politicians, who demanded that pilots fly above a certain height to minimize casualties, thereby degrading the effectiveness of information systems.

- Total information superiority was manipulated, if the debate over the total number of tanks destroyed is any indicator, by asymmetric offsets (e.g., fake tanks, other decoys) and by a study of NATO air operation templates.

- Total information superiority did not result in NATO communications working without serious problems, even after years of practice and in the face of no radio-electronic counterattacks.

During the air campaign over Yugoslavia and Kosovo, NATO had information superiority. But as the discussion above demonstrates, if analysis is inadequate, then information superiority is not enough. One danger in information superiority, then, is in assuming knowledge. Another danger, as the 99.6 percent figure demonstrates, is in overestimating our abilities.

If applied against the major criteria of reducing uncertainty, providing a more complete intelligence picture of the battlefield, and assisting precision-guided missiles in acquiring and destroying targets, information superiority passed many but failed some critical tests in Kosovo (as battle damage assessment showed). We may possess information superiority, but we often fail to exploit it because we can't always correctly interpret what we gather. As a result we are unable to lower uncertainty.

Three problems deserve to be highlighted. First, the methodologies we are using to evaluate data appear to have minor shortcomings which sometimes result in horrific mistakes that directly affect our credibility at higher levels. That is, incorrect assessments by low-level data interpreters eventually diminish the credibility of those officials who have to stand before the public and explain the facts and figures. Sometimes this is a result of consumers who press too hard for answers. But had NATO ground troops been inserted into Kosovo before the Finnish-Russian negotiations ended the conflict, two more reinforced mechanized infantry battalions were awaiting them than expected. This miscalculation was due to the inability of information technology systems and analysts to properly assess and interpret what their “total information superiority picture” of the battlefield really showed (and there were cockpit recordings to study). If open-source reports are correct, we destroyed mockups and decoys in many cases, not working armored vehicles. The cost-effectiveness of air power was greatly diminished as a result. Clearly, more emphasis needs to be placed on the art of battlefield visualization.[33]

Second, we are not realistically assessing the conditions under which our military capabilities are being employed. What was “combat” directed against in Kosovo? Stationary objects, such as buildings, civilian infrastructure, press and police headquarters, and military garrisons; and mobile targets that moved mainly at night if at all, such as tanks, armored personnel carriers, and artillery units. It was not face-to-face combat, but combat conducted from afar. Perhaps "engagement" would have been a better choice of words than combat, although no pilot would agree! We can do better in realistically assessing and describing the conditions under which our forces are engaged.

Third, the U.S. military must rid itself of a degree of self deception that occasionally appears. The U.S. and NATO forces are good and they know it. But they must do better in their estimates of success, for manipulated figures could lead to unrealizable goals or expectations. This attitude can lead military planners to draw false conclusions about Kosovo, previous conflicts, and consequently future operations. A sober assessment of what went wrong is just as important as seeing what went right. No better example could be offered than the expectation of a repeat of the August 1995 "quick concession" from Milosevic, which left planners unprepared beyond the first few days of the conflict in 1999. Our air power is magnificent, but we are becoming its captive because of exaggerations such as those enumerated in this article. Let air power's success speak for itself; even without exaggeration it is without peer.

Drawing the wrong conclusions, as was pointed out with battle damage assessments, can have dramatic and lethal effects on any intervening force. There is a lesson in this, namely that the human in the link still plays a very important role even in the age of information operations, perhaps a more important one than we recognize. Automated warfare is still a long way off if the problems that developed in the nearly opponentless skies over Kosovo are any indicator. U.S. analysts must hone their methodologies to quickly and correctly interpret the cascading amounts of information that confront them in a conflict situation.

They must consider asymmetries in information-age conflict. Improvements in the art of battlefield visualization or conceptualization, including the vital element of interpretation, must be made. The human interpreter of information is every bit as important as the human user of information.

Future conflicts may be very different from NATO's experience in Kosovo. Future enemies could possess some or all of the following: an adept air force; up-to-date air defense sites; precision-guided cruise missiles that can do to our air bases and planes from standoff positions what we can do to theirs (to include destroying AWACS); and the ability to reach the United States with weapons of mass destruction, precision missiles, or terrorist acts. When these threats confront U.S. and NATO systems, what will information superiority do for us? Will it be even more unreliable when stressed by both nontechnical offsets and technological counters? How reliable will those new estimates be? What will happen when a real information warfare system confronts ours? Will our capabilities be degraded by a quarter, a third, or more?

The Pentagon's top civilian leaders evidently plan to produce an official report on Kosovo, breaking their study into three parts: a deployment-employment group, an intelligence support for operations group, and an alliance and coalition warfare group. It is important that the intelligence support group study the current information superiority dogma to correct some of the faulty data and impressions being generated by both analysts and leaders from the Kosovo conflict. We have to stop ourselves before heading down the wrong "yellow brick road," and instead inculcate the wisdom that people like Admiral Ellis are revealing.

NATO and the United States did almost everything right in Kosovo. Now it is time to assess the little that was done wrong. As the Chinese might say, you can lose in contemporary war in two ways: if you fail to defend your information superiority, or if you become trapped by false information. It is the latter to which we should now pay attention.

[1] U.S. Joint Chiefs of Staff, "Information Operations," March 1999, p. 1. Information superiority is based on dominance in three areas: intelligence (with surveillance and reconnaissance support), C4 (command, control, communications, and computers), and information operations.

[2] *Ibid*., p. 6.

[3] "Joint Statement on the Kosovo After Action Review," presented by Secretary of Defense William S. Cohen and General Henry H. Shelton, Chairman of the Joint Chiefs of Staff, before the Senate Armed Services Committee, 14 October 1999. Downloaded from the Internet, DefenseLINK news, http://www.defenselink.mil:80/news/Oct1999/b10141999_bt478-99.html

[4] Julian Borger, "Cyberwar Could Spare Bombs," The Guardian, 5 November 1999, p. 17.

[5] *Ibid*.

[6] U.S. Joint Chiefs of Staff, Joint Publication 3-13, *Joint Doctrine for Information Operations* (Washington: GPO, 9 October 1998), p. GL-7.

[7] U.S. Joint Chiefs of Staff, Joint Publication 2-01, *Joint Intelligence Support to Military Operations* (Washington: GPO, 20 November 1996), p. III-2.

[8] *Ibid*.

[9] "Joint Statement on the Kosovo After Action Review."

[10] Phillip S. Meilinger, "Gradual Escalation," *Armed Forces Journal*, October 1999, p. 18.

[11] Dana Priest, "Air Chief Faults Kosovo Strategy," *The Washington Post*, 22 October 1999, p. 14.

[12] Wesley K. Clark, "The United States and NATO: The Way Ahead," *Parameters*, 29 (Winter 1999-2000), 11.

[13] Discussion with a British defense analyst. The comment is his, not the author's.

[14] William Matthews, "Clark: Kosovo Attack Set Standard for Waging War," *Navy Times*, 12 July 1999, p. 13.

[15] Hearst Newspapers, “NATO Chief: Targeting Goals Leaked to Yugoslavia,” *Pacific Stars and Stripes*, 13 August, 1999, p. 1.

[16] Bradley Graham, “War Review Extended a Month,” *The Washington Post*, 15 September 1999, p. 23.

[17] “Airstrikes Hurt Serb Military Less than Initially Believed,” *The Kansas City Star*, 17 September 1999, p. A16.

[18] David A. Fulghum, “Pentagon Dissecting Kosovo Combat Data,” *Aviation Week and Space Technology*, 26 July 1999, p. 68.

[19] Richard J. Newman, “The Bombs that Failed in Kosovo,” *U.S. News & World Report*, 20 September 1999, pp. 28-30.

[20] Andrew Gilligan, “RAF Admits Failings in Kosovo Inquiry,” *The London Sunday Telegraph*, 25 July 1999.

[21] Frederick Bonnart, “NATO Has a Duty To Be Truthful,” *International Herald Tribune*, 1 October 1999.

[22] *Ibid*.

[23] William S. Cohen, International Institute for Strategic Studies, Hotel del Coronado, Coronado, California, 9 September 1999, downloaded from the Internet (OSD/PA news release), http://www.defenselink.mil:80/news/Sep1999/b09101999_bt409-99.html

[24] *Ibid*.

[25] Paragraph is based on a discussion with Dr. Jacob Kipp, Foreign Military Studies Office, 30 September 1999.

[26] Elaine Grossman, “U.S. Commander in Kosovo Sees Low-Tech Threats to High-Tech Warfare,” *Inside the Pentagon*, 9 September 1999, p.1.

[27] *Ibid*.

[28] *Ibid*.

[29] Mark Danner, “Kosovo: The Meaning of Victory,” *New York Review of Books*, 15 July 1999.

[30] “DARPA Tackles Kosovo Problems,” *Aviation Week and Space Technology*, 2 August 1999, p. 55.

[31] *Ibid*.

[32] *Ibid*.

[33] The subject of battlefield visualization is addressed in the pamphlet “Information Operations” produced by the U.S. Army Information Operations Division, 1999, p. 11.

Lieutenant Colonel Timothy L. Thomas (USA Ret.) is an analyst at the Foreign Military Studies Office, Fort Leavenworth, Kansas. He has written extensively on information operations and on current Russian military-political issues. During his military career he served in the 82d Airborne Division and was the Department Head of Soviet Military-Political Affairs at the U.S. Army's Russian Institute in Garmisch, Germany.

PART FIVE

INTRODUCTION

The United States military is far ahead of the armed forces of the rest of the world in preparing for war in the Information Age, but American military strategists and planners are not alone in pondering the military potential and implications of advanced information and communication technologies. This section presents perspectives on these issues as seen from France, the United Kingdom, Russia, and China.

In the first article, “Information Technology and Military Affairs: France, the United Kingdom, and NATO,” Danielle Phillips argues that the force postures of NATO’s European members “will not be able to meet the requirements of the American conception of 21st century warfare.” Phillips points to several reasons for this conclusion. Differing viewpoints and policies on information warfare and information operations is one, and disagreement about the impacts of advanced technologies on military affairs is another. Significantly reduced European military budgets and the implications of Europe’s growing emphasis on a European Security and Defense Identity, in Phillips view, also present challenges to the abilities of European militaries to maintain pace with that of the United States in moving forward with the revolution in military affairs.

Phillips believes that the United Kingdom’s perspective on information warfare, information operations, and the impacts of Information Age technologies on military affairs is most akin to that of the United States. The United Kingdom's approach "accepts the reality of immense change," and it is "at the beginning stages of formalizing information warfare and information operations doctrine." It is also pursuing weapons programs that will "incorporate weapons and capabilities that will require such doctrine into its defense inventory." Nevertheless, it trails significantly behind the United States.

Meanwhile, in France, views and policies on such issues are also evolving, though more slowly. However, Phillips maintains that France's military modernization efforts are concentrating more on "improving existing capabilities than on developing new generations of weapons that have potential to transform the way that wars are fought." Even so, many in France, Phillips says, feel that "information warfare…is one of the essential instruments in France's sovereignty and independence."

But there is a limit, in Phillips eyes, to how far France has traveled down this road. The thrust of France's efforts is focused mainly on the role of advanced information and communication technologies in commerce, the economy, and society, she says, and France "has yet to publicly incorporate an information warfare strategy into its overall defense program." Overall, she believes that the French position on information warfare and information operations is "a study in contrasts."

Phillips uses the differences between the French and British positions, and in turn the differences between these two countries' positions and that of the United

States, to paint a potentially gloomy picture of NATO's future. The distance between the U.S. and its European counterparts with regard to information warfare and information operations is "immense," she posits, and with the possible exception of the United Kingdom, will continue to grow. She sees this as dangerous for NATO, and advocates that NATO's European states develop a unified approach to information warfare and information operations to forestall this. Nevertheless, as already noted, she fears that if the gap between European and U.S. capabilities continues to grow, "the force posture of NATO's European members will not be able to meet the requirements of the American conception of 21st century warfare."

In this section's second article, "The Russian Understanding of Information Operations and Information Warfare," Timothy L. Thomas observes that even though there are numerous similarities between U.S. and Russian approaches to information operations, there are three distinct differences between Russian and U.S. views of information warfare. First, Thomas, says, the fact that Russia is experiencing a massive transformation of all aspects of society influence Russian analysts to place a much greater emphasis than U.S. analysts on "information-psychological processes" as components of information warfare. Second, since Russian military thinking has been historically different than Western thinking, Russian military analysts naturally place different emphases on different aspects of information warfare than do Western analysts. Finally, Thomas asserts, Russian views of information warfare are different than their Western counterparts because of the budgetary, technological, and infrastructure constraints under which Russia labors.

Thomas begins his analysis of Russian perspectives on information operations and warfare by discussing Russia's 1995 draft law on information security. It lists critical areas of information security as the information resources of the Russian Ministry of Defense, the military-industrial complex, the country's overall command and control system, the political-moral condition of the armed forces, and the country's overall information infrastructure. External threats to these critical areas are identified as all types of foreign intelligence activities, electronic warfare and computer intrusion, psychological operations of probable enemies through special means or mass communications, and the activities of foreign political or economic structures working against Russia's interests.

Thomas next turns his attention to Russian definitions of information warfare. He provides several definitions, synthesizing them into "ten key elements of the Russian approach" to information warfare. First, most Russian analysts agree that there are "natural laws and principles" associated with information warfare, although they disagree on whether the laws have been identified. Second, most Russian analysts agree that information warfare is conducted during peace and war, with IW operations in peace being conducted primarily covertly. Third, Russian approaches to IW focus on its "information-psychological" aspects, that is, the impact of information on members of society. Thomas labels this as "perhaps [the] primary difference" between the Russian and U.S. approach. Fourth, Russia is engaged in serious attempts "to harness the energy generated by human beings" to affect information operations and information warfare. Fifth, Russian analysts believe information operations have geo-strategic significance. Sixth, Russia calculates the information potential of a country as a measure of that country's military power that is information based. Seventh, information operations, to some Russian analysts, greatly affect the study of military art. Eighth, Russian research and development in computer and information sciences is producing some results unique to the Russian experience such as the "neuron computer." Ninth, somewhat similar to the U.S. concept of the "system-of-systems," Russian scientists are devoting more attention to the interaction of combat systems. Finally, to almost all Russian analysts, information is likely to become one of the most likely spheres of military confrontation.

Despite his identification of these ten key approaches, Thomas hesitates to draw conclusions about their implications. Noting that Russia "does not appear to have a clear idea where it will end up" regarding information warfare, he advocates the need to pay close attention to the evolution of Russian thinking on information operations and information warfare. This is sage advice, especially if, as Thomas believes, there are those in the Russian military who believe that the West will use its information capabilities to "further its control over Russia."

Conversely, M. Ehsan Ahrari exhibits no similar hesitancy to present conclusions in his "Information-Based Warfare and the PRC." Ahrari argues that China has carefully watched the development of U.S. information warfare capabilities during and after the Gulf War and itself is determined to emerge as a dominant power in the Asia Pacific region. Ahrari also believes that the Chinese military has been heavily influenced by U.S. information-based warfighting techniques and is moving as rapidly as it can to include information-based capabilities in its inventory.

Ahrari presents evidence that Chinese analysts see information as a “prime strategic resource in warfare,” and also stresses that many Chinese analysts believe that warfare in the Information Age will require restructuring of the Chinese military. Ahrari believes the Chinese military may move to a decentralized command and control structure.

The Chinese military is also aware of China’s vulnerability to information war, Ahrari says. Computer viruses and attacks from the Internet launched by “a child’s prank or an attack from an enemy” are items of special concern. Enhancing computer security is a central concern of Chinese analysts, according to Ahrari.

Ahrari concludes with three separate observations. First, he stresses that even though China wishes its military “to emerge as a high-tech warfighting machine,” it presently presents “absolutely no threat to the United States armed forces.” Second, he emphasizes that this reality should not influence anyone “to forget the current Chinese commitment” to develop such capabilities. Finally, he also argues that China’s smaller neighbors must watch China’s military modernization in information warfare and other areas as well and “try not to remain too far behind.” This caution is designed to assure that other East Asian states can counter the concern that Ahrari raised at the outset of his analysis, that China is determined to become a dominant power in the Asia Pacific region.

In this section’s final article, “The Third Military Revolution” Ch’en Huan presents his view that with the development of information technology, stealth technology, and long-range precision strike technology, a third military revolution has occurred that will have “far-reaching effects on military practice and theory.” Ch’en Huan argues that the new technologies are forcing the traditional military principle of concentration to be re-examined. Indeed, the author maintains that it is no longer necessary to strike an enemy’s concentrated forces, but rather it is best to strike and destroy his information since such an approach could “achieve the operational objective of paralyzing the entire body” of the enemy’s force. At the same time, Ch’en stresses that it is necessary to defend and preserve one’s own information so as not to become paralyzed.

This, Ch’en believes, means that warfare is moving from an era in which physical weapons dominated to one in which “cerebrum counter-measures” will dominate. He also believes that “nonlinear attacks on enemy objectives” will lead to a blurring of lines between the front and the rear in warfare. New operational concepts such as “long-range combat,” “outer space combat,” and “paralysis combat” will rise rapidly, making armed forces that are not prepared for rapidly changing forms of combat especially vulnerable to defeat.

Ch’en’s discussion of “paralysis combat” is especially interesting. Building on his earlier theme that it will not be necessary to destroy an enemy’s forces, the author points to “computer combat,” “radiation combat,” and “robot combat” as emerging effective ways to paralyze one’s enemy without necessarily taking on his main military forces. At the same time, he asserts, the Information Age will require a “thin and flat” command structure. “Operational simulation” will also become a larger part of the military's repertoire. Finally, Ch'en believes that Information Age technologies will result in smaller militaries that will be internally divisible in more ways than today's militaries. The future military will have units that "can at will be divided and combined" "based on the nature and need of an operational mission."

While none of these views of the nature of warfare or the military in the Information Age is radically different than those offered in the United States, even small differences may be worthy of note. In the 1930s, the difference between the French and German approaches to the use of tanks appeared insignificant. French tanks were attached to infantry divisions for troop support, while German tanks were organized into highly mobile panzer divisions. The first few days of World War II showed that this difference was anything but insignificant.

Is a similar phenomenon developing with information warfare, and if so, what is it? It is too soon to tell, but not too soon to examine different approaches to information operations and information warfare to see if seemingly insignificant differences in fact may have immense importance.

CHAPTER 22

INFORMATION TECHNOLOGY AND MILITARY AFFAIRS:

FRANCE, THE UNITED KINGDOM, AND NATO

By
Danielle Phillips

Throughout its history, NATO has based its defense planning and policies on the shared outlooks of and close cooperation between the political leadership and defense establishments of its member states. Cooperation has never been perfect, and outlooks have never been identical, but in the history of alliances, few have been as cooperative, as long-lasting, and as successful as NATO.

Formed primarily to deter and if necessary defeat feared Soviet aggression, NATO since the collapse of the U.S.S.R. has reinvented itself. Thus, at the April 1999 NATO Summit in Washington, held on the 50th anniversary of the founding of the organization, NATO adopted a new Strategic Concept that moved beyond the old conception of collective defense and encompassed comprehensive crisis management. Henceforth, NATO will not only defend its member states, but also move against threats to the values that it espouses in areas of interest and importance to its member states. *Operation Allied Force*, the air war in the skies over Kosovo and the former Yugoslavia in 1999 in opposition to Serbian ethnic cleansing against Albanian Kosovars, was the first operational manifestation of the new doctrine.

Having withstood and surmounted the dangers of the Cold War and redefined its primary purpose for existence in the post-Cold War world, NATO in the early 21st century is the world's pre-eminent alliance. Nevertheless, it faces an insidious internal challenge born of the technologies of the Information Age.

That challenge results from the significantly different approaches some NATO member states are taking to what is called in the United States the "revolution in military affairs" (RMA), and to the diverging military capabilities that are developing within NATO as the result of different speeds and levels of application of the technologies of the RMA to different militaries. Much of the challenge results from differing viewpoints and policies on information warfare and information operations, and differing views on the impacts of advanced information and communication technologies on military affairs.

Indeed, as successful in an operational sense as NATO was in *Operation Allied Force*, the existence both of different approaches to Information Age warfare and of different levels of military capabilities was discernible there. Put simply, the United States shouldered the brunt of the burden of the air war at least in part because the military capabilities of other NATO states could rarely be integrated with the operational requirements of U.S. forces. It would be ironic—and unfortunate—if the technologies of the Information Age proved to be the instruments of the decline of NATO.

Bounding the Issue

NATO's political leadership and planners are aware of the challenge and are attempting to address it. Indeed, at the December 1998 NATO Defense Ministerial Meetings, NATO defense ministers agreed to develop a defense capabilities initiative for the 1999 Washington Summit. The proposed initiative aimed at "developing a common assessment of requirements for the full range of military operations with a particular emphasis on technology and interoperability, especially in areas such as logistics and command, control, and communications." It also proposed to address "capabilities which are critical to the successful execution of joint military operations."[1]

The language of the guidance did not make specific reference to information warfare, information operations, or the impacts of advanced information and communication technologies on military affairs. However, considering *U.S. Joint Vision 2010* and U.S. Secretary of Defense William Cohen's pre-ministerial push for NATO to examine its information technology capabilities, one can infer that information warfare and information operations were central issues at the root of this guidance.[2]

After the 1998 Ministerial, NATO at its 1999 Washington Summit detailed a new Strategic Concept and Defense Capabilities Initiative.[3] These are steps in the right direction. However, it is far from certain that the potential of either will be fully realized. Within NATO, there are significantly different views on many issues regarding the RMA and its implications, not the least of which different views concerning information warfare, information operations, and the impacts that Information Age technologies will have on military affairs.[4]

Indeed, the belief that an information technology based revolution in military affairs is well underway and advancing rapidly is primarily held in the United States, and to a similar but lesser degree the United Kingdom. The concept of an RMA is often met with hesitation, skepticism, and even outright resistance by many of NATO's European members.

At the same time, NATO is expanding its sphere of influence and increasing its operational reach just as its member states are experiencing across the board reductions in defense spending and military capabilities. A number of NATO nations have revised their national defense strategies to take into account the radically different international security environment and the need for force modernization in light of Information Age technologies. Even so, the degree to which individual national defense thinking and capabilities are being modernized varies from state to state.

A few states, led by the United States and to a lesser degree Great Britain, have accepted the RMA as the inevitable wave of the future of warfare. They are incorporating advanced Information Age technologies into their armed forces at moderately high to extremely high rates of speed. They also are adapting their tactics, operations, and military doctrines to those technologies and the capabilities they provide, even if more slowly than the more forceful advocates of the RMA would prefer.

Other states, notably France and many smaller NATO nations, are proceeding more slowly still, both in the rate of incorporation of new technologies and in the adaptation of tactics, operations, and doctrine. Some do not accept conceptually or philosophically that an RMA driven by advanced information and communication technologies is in the offing. Others see in the post-Cold War world advantages in developing a separate European security and defense identity with European-oriented security and defense strategies and doctrines. Almost all are constrained in the amount of new technology they can incorporate in their militaries because of reductions in military budget.

For NATO, this is potentially dangerous. To the extent that different NATO states obtain different military capabilities and adopt different strategies and doctrines based on those different capabilities and different views of the future of warfare, the shared outlooks and close cooperation that bound NATO together during the Cold War have potential to diminish during the early years of the Information Age.

To reiterate, as successful in an operational sense as NATO was in *Operation Allied Force*, the beginning of such a phenomenon was discernible there. It would be ironic—and unfortunate—if the technologies of the Information Age proved to be the instruments of the decline of NATO. This study will explore this challenge in several ways.

First, it will examine the perspectives and policies of two European NATO states, the United Kingdom and France, on information warfare, information operations, and the role and impacts of Information Age technologies in and on warfare. Given that these technologies are central to the economic transformations taking place in the United Kingdom, France, and other European states, the study will also explore some of the changing interrelationships between defense industries, military establishments, and advanced information and communication technologies.

Second, the study will also assess the implications of those perspectives and relationships for NATO's future. Unless handled carefully and correctly, the presence of significantly different outlooks and undertakings on information warfare and information operations within and between NATO's 19 nations has potential to weaken if not disrupt the alliances ability to function.

Finally, the article will conclude with a set of recommendations designed to help NATO maintain its cohesion as the alliance moves deeper into the Information Age.

The United Kingdom: Views and Policies

Of all of NATO's European members' viewpoints and policies on information warfare, information operations, and the impacts of advanced information and communication technologies on military affairs, the United Kingdom's perspective is in most respects the closest to that of the United States. From the British perspective, the biggest change in the conduct of future military operations is likely to come from a combination of improved weapons and weapons capabilities and from the application of information technology to military command and control.[5] This in turn, official British spokesmen maintain, has potential to transform the way that 21st century wars will be fought.

Doctrine, Policy, and Programs

This perspective developed over time, but was finally codified in 1998 when the United Kingdom concluded its *Strategic Defense Review*. The review marked a significant departure from the United Kingdom's previous defense posture. Under the auspices of the 1998 review, the United Kingdom is pursuing a program of force modernization that will develop new generations of weapons that incorporate Information Age technologies. The incorporation of Information Age technologies into the military structure is part of the British Ministry of Defense's plan to develop an efficient, top-of-the-line, cost-effective force posture.

The *Strategic Defense Review* identifies a number of military capabilities as important to force development. Among the most prominent in the British strategy are those associated with information warfare and information operations, especially command, control, communications, and computers. The British also see intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) as critically important. Some of the capabilities contained within the new force posture include the Airborne Standoff Radar Surveillance System (ASTOR) and an indirect fire precision attack program including "smart, long-range, guided weapons delivered by rockets or extended range artillery."[6] The British program also incorporates increased use of stand-off weapons and unmanned platforms such as unmanned vehicles for aerial reconnaissance and the removal of mines on land and at sea.

The British are also taking steps to address potential weaknesses resulting from increased reliance on technology. For example, recognizing that "increased automation of tasks" can increase vulnerabilities by reducing the situational awareness of human operators, the British have implemented programs designed to train and educate personnel involved with advanced technologies.[7] In addition, the United Kingdom has initiated programs such as the Joint Battlespace Digitization initiative, which is designed to "improve operational effectiveness by integrating weapons platforms, sensors, and command, control, intelligence, and information systems." It is based on the belief that in the future, military operations will be merged into joint operations rather than take place in separate battlespaces under the domain of individual armed services.[8]

In light of these advancing military capabilities and the perceived changing face of battle, the British military also recognizes the need for doctrinal evolution to maintain overall force effectiveness. To accomplish this, Ministry of Defense officials are working in close conjunction with the U.S. Department of Defense to explore and to further develop policy and doctrine for the United Kingdom's evolving national security and defence policy strategy.

The British Ministry of Defense is confident that it can incorporate Information Age capabilities into its national security posture despite a downward trend in British defense expenditures. One way to accomplish this is by incorporating off-the-shelf civilian and commercial capabilities into military equipment, especially in the areas of information and communication technologies. The British defense establishment recognizes that with “civil investment in research and development 10 × greater than [that of] defense investment” in the fields of electronics, software and information technology, “new advances in the civil market are increasingly having profound implications for [their] future military capability.”[9] This is a significant change from the traditional British (and American) pattern in which capabilities developed by the military were later transferred to the private sector.

The Defense Industrial Sector

Indeed, the United Kingdom has formally adopted this changed perspective as formal policy. Thus, guided by the *Strategic Defense Review*, the United Kingdom also established a Defense Diversification Agency designed to promote civil-military joint ventures, research partnering, and development of dual use technologies. One of the chief target areas for the agency is information and communication technologies.

The objective of the Agency is not only to incorporate advanced Information Age technologies into British weapons and defensive systems. It also clearly seeks to help British industry. Since the mid-1980s, British defense spending has been cut 33 percent. These reductions have impacted not only overall defense policy, but the British defense industrial base as well. The Defense Diversification Agency aims to preserve and promote British defense industries through a civil-military program of technology transfer designed to “get the most out of defense technology.”[10] The British clearly feel that the defense industry should diversify and adapt to the changing security and economic environment.

The Defense Diversification Agency will promote dual-use research and a formal system of technology transfer between the private commercial sector and the military. It will not only promote the incorporation of civilian technologies into military capabilities, but also the diffusion of military technologies into the private sector. The agency plans to develop a database containing "a wealth of knowledge within MOD about future equipment needs, about technological trends, about sources of advice and assistance, and about relative market assessments." This knowledge will be made available to companies so that they can "exploit potential new opportunities for their products, technologies, and skills in the UK and overseas military and civil markets."[11]

The Defense Diversification Agency also makes provisions for a Defense Diversification Council chaired by a prominent industrial leader, "with a membership drawn predominantly from industry but including also the Chief Executive of DERA and other appropriate representation from central and local government and from trade unions."[12] In addition, the Agency will create Technology Diversification Managers who will work directly with local industries to "build a collaborative relationship in order to 'broker' technology activity between DERA and local small and medium enterprises."[13]

Overview

Clearly, the United Kingdom's approach accepts the reality of immense change, even an RMA, in military affairs and economic affairs driven by Information Age technologies. Although the United Kingdom is only at the beginning stages of formalizing information warfare and information operations doctrine, it is pursuing programs that will incorporate weapons and capabilities that will require such doctrine into its defense inventory. It has also identified a strategy and created an organization that aims to harness and incorporate the best civilian technologies into military capabilities, thereby ameliorating the impact of the drawdown in its defense budget. It has created and is implemented training programs designed to enhance the ability of British soldiers, sailors, and airmen to master new required skills. The United Kingdom, in other words, appears to have accepted the inevitability of an RMA driven by Information Age technologies, and is adapting its defense posture accordingly.

France: Views and Policies

France's views and policies on information warfare, information operations, and the impacts of advanced information and communication technologies on military affairs are also evolving. However, they are evolving more slowly than the United Kingdom's views and policies, and in certain important respects are markedly different from those of the United Kingdom. Even though France is not a participant in NATO's integrated military structure, its views and policies on these issues are vitally important for several reasons.

First, France is a major player in European affairs and global military affairs, and its outlooks and positions carry significant influence on the continent. Second, France's involvement in NATO military affairs significantly increased during the 1990s. In the post-Cold War world, France has again become a critical player within NATO. Third, France is one of the leading promoters of the European Security and Defense Identity (ESDI) within the European Union. ESDI carries significant importance for both the EU and NATO. And finally, France's defense industries are pillars of Europe's defense industrial capacity, and French science and technology and its application to weapons and defense systems has long been at the forefront of European and global military affairs. Thus, the French perspective on information warfare, information operations, and the role of advanced information and communication technologies in the military can not be overlooked.

Doctrine, Policies, and Programs

Like the United Kingdom, France is pursuing a program of force modernization. However, at least rhetorically, France's modernization efforts concentrate more on improving existing capabilities than on developing new generations of weapons that have potential to transform the way that wars are fought. Many in France feel that "information warfare [and information operations—author] is one of the essential instruments in France's sovereignty and independence, one of concern not only to the defense industry, but also the economy, media, science, and culture."[14]

Many in the French defense establishment recognize the importance of developing an information technology strategy, but this recognition does not necessarily carry over into a publicly stated intention to develop an information warfare or information operations strategy. The thrust of French efforts appears focused mainly on the role of information and communication technologies in commerce, the economy, and society, not defense. Although France's overall concept of information warfare falls in line with American schools of thought, France, unlike the United

States and the United Kingdom, has yet to publicly incorporate an information warfare strategy into its overall defense programming.

Nevertheless, French military planners and thinkers are well aware of the need to accelerate their planning and preparations for new types of warfare. As long ago as 1996, senior French defense and armaments industry officials began to become concerned that France was lagging behind on the information warfare front. General Jean Philippe Douin, former Chief of Staff for the French Armed Forces, announced in an internal memo that "a new type of warfare was coming to the fore."[15] To remain competitive at the industrial level as well as in security circles, he posited, France needed to seriously examine its information technology capabilities and develop a coordinated information warfare strategy. Shortly thereafter, the Centre d'Electronique de l'Armement (CELAR) officially assumed the lead for French information warfare strategy.

By the late 1990s, CELAR had become France's "technical center of the war of information for defense."[16] However, CELAR's primary research and development activities lie in the traditional areas of electronic and optronic warfare. Thirty eight percent of its work is dedicated to these fields, with 8 percent designated to optronic and electronic component development. Other areas in which CELAR specializes are information systems, telecommunications, and information system security. Only 33 percent of this work focuses on information and communication systems combined, while the remaining 21 percent is dedicated to security.[17]

However, even though CELAR has an input in all programs involving information technology, it does not actually set information technology strategy, nor does it have authority over other agencies that work on information technology or information warfare issues. Thes other agencies include the Direction des Affaires Strategiques (DAS) and the Ecole Polytechnique's Centre de Recherché et d'Etudes Scientifiques et Techniques (CREST). Each agency acts individually, with little to no harmonization of efforts. Through at least 1996, there was "no official body to dovetail all the [infowar] undertakings, leaving each organization to work in relative isolation" on issues of information warfare and information operations.[18]

Despite these impediments, information warfare and information operations have arguably gained greater importance in French defense thinking and policy. By the end of 1997, the technology used by the French military had become increasingly similar to civilian capabilities, indicative of a recent migration toward the incorporation of civilian technologies into the military structure.[19] In 1998, the French army began to increase its focus on incorporating improved information and command systems into its structure.[20] Although French spokesmen have inferred that one of France's ultimate goals with regard to information capabilities is to be able to glean real-time information and deploy resources and forces to meet threats as soon as possible, this is not necessarily an information warfare or information operations strategy.

As intimated above, France's recent steps forward in thinking about and planning for information warfare and information operations have been translated into defense programs in only a limited way. France's defense program remains based on a strategic vision for national defense enunciated in 1995, before the more recent emphasis on the role of Information Age technologies in warfare. Designed to look 20 years into the future, France's 1995 defense programming bill redefined the role and structure of the armed forces as well as the concept of French national security as a whole. Developed to address France's changing security and defense needs in the context of the evolving international security environment, France's programming bill outlined four strategic components of national defense: protection, deterrence, prevention, and projection. None of these clearly embraced information warfare or information operations concepts or capabilities.[21]

"Protection" concentrated on the defense of French territory. Major components consisted of controlling the trilateral approach to territorial defense, development of surveillance, and protection against threats.

"Deterrence" is "at the heart of France's defense strategy." It relied and relies on two "reduced and modernized components:" a submarine capability and an air capability.

"Prevention" of conflict revolves primarily around political actions. However, it involves military aspects as well, including intelligence, technical cooperation, and pre-positioning of forces.

"Projection" of power involves rapid deployment of forces outside France's national territory. It includes a stated need to attain the capability to deploy quickly a land component outside France of over 50,000 troops for NATO operations or 30,000 in a main theatre. It also includes a naval force projection capability of a "service group with its backup and a submarine force over a distance of several thousand kilometers," and air projection of an “air transport capability maintained at the current level, [which is approximately] 100 combat aircraft and the corresponding refueling aircraft, air traffic control and detection means, and two air bases.”

In comparison to France’s past force structure, these four objectives are to be achieved by a radically altered military structure. Most noticeably, the size of French armed forces will be drastically reduced.

By 2015, the French army will be reduced from a 1995 level of 271,500 to 170,000, a 37 percent reduction.[22] The French army will reduce its organizational structure from nine to four divisions, with as many as 38 operational regiments set to be disbanded by 1999.[23] However, it plans to incorporate field surveillance and data processing equipment to reinforce its “balanced division of heavy tanks and light tanks supported by Tigre helicopters, along with an increased range in precision of long-range weapons.”[24]

Likewise, the French Navy will be reduced by approximately 20 percent, and the air force by slightly more than 25 percent. In addition to reductions in manpower, the navy will undergo a reduction in tonnage and number, as 13 ships will be decommissioned early. The Air Force will concentrate on projection capabilities and adopting new operational modes. Various groups within the air force will be disbanded by the end of 1999, including the Albion First Strategic Missile Group, the surface to surface ballistic nuclear component, and the Toul-Thouvenot air engineers regiment and support base. The Toul-Rosieres and Contrexeville air bases will be transformed into air detachments.[25]

As this transpires, France plans to embark on improved training, incorporating a plan of military professionalization, gradually phasing out compulsory service and consolidating military equipment and organizational structures in each sector of the armed forces. The goal is to create a small, efficient, effective military.

However, unlike Britain's program, the French program appears to concentrate more on upgrading old systems and introducing advanced versions of already deployed systems. For example, included among the 1999 defense budget projects are the modernization of 13 Eridan class minesweepers, the development of improved air to surface missiles with improved propulsion and guidance capabilities (the ASMP), and the renovation of the command and control systems for a number of aircraft.[26] Thus, the French defense plan is instructive as much for what it does not say as for what it does say. It includes few new weapons systems or defense capabilities that are heavily dependent on new Information Age technologies.

France's 1999 military research and development budget provides a good case in point. While the 1999 defense budget designates 5.485 billion French francs for research and 15.604 billion francs for development, there is no publicly specified designation for the new information warfare related capabilities. Nor is there any reference to development of new revolutionary types of warfare, either operationally or in doctrine and strategy. Instead, France's modernization appears to focus on more traditional improvements in areas such as electronic and aerospace warfare, as well as improving existing capabilities rather than developing new ones.

The Defense Industrial Sector

This is evidenced not only by budgetary trends, but also by the publicly stated goals of the newly restructured defense industry. This restructuring was necessitated by the need to adapt to the drastic cuts France has made in its overall defense budget. Indeed, the restructuring of France's national defense industry is actually one of the components of France's overall defense strategy. The government has identified three fundamental goals to be achieved through the restructuring:

1. preserving "the integrity of industrial, technological, and human capital whilst developing essential synergies; preserving the interest of national defense;"

2. opening "new development perspectives;" and

3. pursuing and reinforcing "the policy of alliances, reunions, or fusions which have already taken place on a European level."[27]

This redesigned defense industry is intended to serve as a vital player in France's modernization effort economically, industrially, and politically. The privatization of Thomason SA, the 1998 merger of Dassault Aviation and Aerospatiale, and the 1999 merger of Aerospatiale and Matra to form Aerospatiale Matra evidence the French commitment to restructuring the defense industry in order to remain competitive regionally and globally. Though the new face of the French defense industry is to be "a government reinforced industrial structure, particularly in the field of high technology," the main focus thus far has primarily been in the fields of aerospace, aeronautics, and electronics, not advanced information and communication technologies.[28]

The promotion of French and European defense industries is a byproduct of the European Union's European Security and Defense Policy. France in particular would like EU members to develop the security structures and military capability to conduct crisis management operations on its own if the United States and NATO opt not to become involved. For this to become a reality, a strong, unified defense industrial base is needed.

Inherent in this concept is a degree of increased independence from the United States both at the security planning and the defense industrial levels. In 1997, France joined the United Kingdom and Germany in identifying and implementing a trilateral initiative to promote the competitiveness of European defense industries to serve as a David to the United States defense industries' Goliath. One of the primary objectives in merging DASA and Aerospatiale Matra, as well as the other defense industrial consolidations that swept across Europe in 1999 was to create a defense base that could successfully compete with U.S. defense industrial rivals.

This initiative may be beginning to bear fruit. In the late 1990s, France began to increase its development of information warfare capabilities at the industrial level. Dassault in particular has made major contributions in terms of battlefield knowledge and rapid information processing. Yet the French defense industry has only minor influence on the overall state of defense policy, at least with regard to information warfare. Major defense contractors such as Thomson, Matra, Alcatel, Giat Industries, and Dassault "are represented by just a single consultative and largely informal committee."[29]

Overview

France, then, presents a study in contrasts in its positions on information warfare, information operations, and the impacts of advanced information and communication technologies on military affairs. French military leaders and thinkers are fully aware that major changes are taking place in the conduct of warfare, many driven by Information Age technologies. Nevertheless, at least in public, the French Ministry of Defense has yet to develop and incorporate information warfare and information operations doctrine, strategy, and tactics into its overall defense planning. While France has gradually come to recognize the importance of information warfare and information operations, the fruits of this recognition have yet to ripen despite a recent acceleration in this regard. To reiterate, then, when compared with the United Kingdom and the United States, it is apparent that the critical issue for France is not so much what has done with regard to information warfare and information operations, but what has not been done.

Implications for NATO

The differences between British and French perspectives and policies on information warfare and information operations are indicative of those that exist among and between other NATO members as well. In addition, many smaller NATO states have neither the economic wherewithal nor the technological capability that might allow them to incorporate significant quantities of Information Age technologies into their military forces. This, in turn, acts as an inhibitor on doctrinal, strategic, operational, and tactical change. As we have seen, this is the case even in a country such as France that has a highly developed technological, industrial, and military base.

This could create serious difficulties for NATO as it attempts to structure and organize its forces and capabilities for 21st century contingencies. Thus, while France recognizes the military importance of advanced information and technologies, it has yet to fully integrate them into its military strategy, doctrine, or forces. Conversely, the United Kingdom and the United States are molding defense strategy around advances in Information Age technologies. To reiterate, it is not necessarily what the French have said and done, but rather what they have not said and done.

What does this mean for NATO?

If advances in information technology are in fact changing the face of military affairs, national military planners must be prepared to abandon traditional thoughts on war and adapt a new defense paradigm. Such a new defense paradigm will contain not only new concepts of military capabilities, but also of organizations and even the very concept of war itself. Therefore, if as prevailing thought in the defense intellectual communities in the United Kingdom and the United States suggests, we are in the midst of a revolution in military affairs driven by information and communication technologies, NATO must revolutionize its thinking and its capabilities to maintain military effectiveness.

The problem with this is that the very nature of NATO force planning is such that NATO cannot dictate defense policies to its member nations. Therefore, if the military capabilities of NATO are to be revolutionized, a revision of the defense strategies and force postures of NATO members at the national levels must occur first.

The problem facing NATO is how national defense ministers and the defense establishments of all of its member nations can be convinced to accept information warfare and information operations both philosophically and conceptually.

But the problem does not end there. Once the defense establishments of NATO's member nations accept information warfare and information operations philosophically and conceptually, they must either increase defense spending or redirect and refocus it toward Information Age technologies that are at the core of the RMA. Given that the downward trend in defense spending since the end of the Cold War is unlikely to be reversed absent an immediate identifiable threat, refocusing and redirecting will undoubtedly be required. And even though information warfare and information operations may be more cost effective than previous types of warfare since civilian and commercial technologies can be incorporated into military postures relatively inexpensively, the initiative to integrate these technologies must first be taken by higher levels of government.

In other words, it must be a top down process. While industries may provide the technological capabilities, they cannot dictate national defense policies. It is thus imperative for industries to have a high level of involvement in the defense planning process if NATO nations wish to successfully incorporate civilian capabilities into military systems. But as we have seen, there are different approaches to this within NATO. While the United Kingdom encourages and facilitates a high level of industry involvement through forums such as the Defense Diversification Council, France incorporates industry only minimally and through largely informal channels.

The degree to which individual NATO nations will be able to involve industry in their defense programs will, in large part, determine the degree to which each nation will be able to develop an authoritative, decisive information warfare and information operations strategy. It will also help determine the degree to which each nation will be able to successfully develop information warfare and information operations capabilities in and of themselves. If there are significant disparities in information warfare capabilities among NATO member nations, the Alliance will arguably face serious problems in terms of overall effectiveness and in terms of interoperability. Therefore, NATO nations need to ensure that their information warfare developments are at least somewhat coordinated. This will no only reduce duplication of efforts, but also ensure the interoperability of forces.

Conclusions

At present, the United States leads NATO with regard to information warfare and information operations capabilities, with the distance between the United States and its European counterparts immense. This is a dangerous situation for NATO. Unless homogenized and coordinated, the different military tracks pursued by members of NATO will inevitably result in significant interoperability problems due to disparities in military capabilities. It will become increasingly difficult to maintain “separable but not separate” forces.

The United States and the United Kingdom are preparing to fight a new type of warfare, with a new class of weapons, with new doctrines. Meanwhile, other NATO states are not pursuing this course of action. The prospect of a NATO operation in which some members are prepared to fight Information Age warfare with state of the art equipment and doctrine, while other members and partners possess only 20th century capabilities is a daunting one which the Alliance must address.

If the United States is leading this revolution, how then can the outlooks, policies, and technologies of the U.S.’s NATO allies and partners be synchronized, if not harmonized, with those of the United States, and for that matter, the United Kingdom?

This is an extremely tricky issue. If not handled delicately and diplomatically, the RMA, information warfare, and information operations affairs could create a divide between “Fortress Europe” and “Fortress America.” A push to bring European Allies up to American standards runs the risks of creating an intellectual divide between the United States and United Kingdom on the one hand and the rest of NATO on the other hand. Similarly, considering the European push to develop ESDI and promote the independence of European defense industries, an effort to “Americanize” information warfare and information operations standards and capabilities could fuel competition between industries. This would undermine rather than promote the national and industrial coordination needed if the alliance is to develop a unified, compatible, and capable information warfare and information operations capability.

Consider for example, the British, French, and German public commitment to creating an independent, competitive European defense industry which would be able to successfully compete against the American giants. While the United Kingdom recognizes U.S. dominance in the field of information technology, has publicly acknowledged that the United States will lead the way in this field, and is prepared to follow the U.S. lead, there is little evidence that other major NATO states are prepared to follow suit. Though the United Kingdom may presently be prepared to embark upon collaborative, coordinated efforts with the United States in information warfare and information operations, continued pressure from other European partners to promote European independence from and competition with American defense industries may place the United Kingdom in a position in which it is forced to choose between the United States and its European partners.

This competition and subsequent uncoordinated development of military capabilities poses a potential defense dilemma not only for the United Kingdom, but also for NATO. NATO states including France are committed to the concept of force and systems interoperability. However, for interoperability to become a reality as new capabilities are brought on line, it is imperative that defense strategists, planners, and industries work in conjunction with one another to develop complimentary and compatible strategies, plans, and technologies, and to avoid a duplication of effort.

At its 1999 Washington Summit, NATO unveiled a Defense Capabilities Initiative designed to improve "interoperability and sustainability among Alliance forces…[and to] ensure that the military forces of the Allies remain on the same wavelength and able to move distances effectively and quickly."[30] The effectiveness of this, or any NATO initiative, is determined by commitment at the national level to making that initiative a reality. In spite of dwindling defense budgets, the European Allies appear to have placed a new emphasis on improving their capabilities and increasing their share of the Alliance's burden.

The political rhetoric to support increasing capabilities has reached new levels in European capitals. This is in large part due to *Operation Allied Force*, in which European deficiencies were glaringly illustrated. As a result, the Allied focus on capabilities has reached a fever pitch—but not in respect to information warfare capabilities. Rather, the capabilities the Europeans have designated with "must have" status are items such as strategic lift, precision guided munitions, and the like. It is important to note, however, that defense budgets have yet to reflect this new trend.

In light of constrained budgets and the EU's commitment to deploying and sustaining a 60,000 man force capable of carrying out Petersberg Tasks by 2003, any marked improvement in capabilities will likely be in support of peace keeping and crisis management missions. It is unlikely to be in areas such as information warfare and other revolutionary battle scenarios. Unless NATO's European members determine that information, communications, and logistics are primary foci of their national defense strategies, and budgetarily commit themselves to developing these capabilities, the force posture of NATO's European members will not be able to meet the requirements of the American conception of 21st century warfare.

[1] NATO Defense Ministerial Press Communiqué. M-NAC-D-2(98)152. December 17, 1998.

[2] At the Department of Defense Concept Development and Warfighting Conference, Cohen publicly advocated NATO modernization and restructuring to develop four core capabilities—mobility, effective engagement, survivability, and interoperability—by "improving command control, and communications, logistics, and interoperability." Cohen also insisted that members should share technological innovations as "a military force is only effective as its flow of information.

[3] See *The Alliance's Strategic Concept*, NATO Press Release NAC-S(99)65, and *Defence Capabilities Initiative*, NATO Press Release NAC-S (99)69.

[4] Linda D. Kozaryn, "NATO Needs More Mobility, Better Ammo," *Defense Press Service News*, November 19, 1998.

[5] *United Kingdom Strategic Defense Review* (London: Ministry of Defense, 1998), p. 37.

[6] *Ibid*.

[7] *Ibid*.

[8] *Ibid*.

[9] *Ibid*.

[10] *Ibid*.

[11] *Ibid*.

[12] *Ibid*.

[13] *Ibid*.

[14] "France Advances on Infowar Front," *Intelligence Newsletter* Volume 289. (June 6, 1996).

[15] *Ibid*.

[16] La Delegation Generale pour l'Armement, at http://www.defense.gouv.fr

[17] "France Advances on Infowar Front," *Intelligence Newsletter*, Volume 289 (June 6, 1996).

[18] *Ibid*.

[19]"Ever Faster Move to Dual Use Tech," *Intelligence Newsletter*, Volume 324 (December 4, 1997).

[20]"Infowar the Star at Eurosatory Show," *Intelligence Newsletter*, Volume 337 (June 18, 1998).

[21]"The Various Aspects of our Defense Strategy," at http://info-france-usa.org/profil/glance/def97/various.htm

[22]"The New-Style Armed Forces," at http://info-france-usa.org/profil/glance/new.htm

[23]"Reorganization of the Forces from 1997 to 1999," at http://info-france-usa.org/profil/glance/def97/reorgani.htm

[24]"The New-Style Armed Forces," at http://info-france-usa.org/profil/glance/new.htm

[25]"Reorganization of the Forces from 1997 to 1999," at http://info-france-usa.org/profil/glance/def97/reorgani.htm

[26]*Annual Report: Le Projet de Budget de la Defense pour 1999* (Paris: September 9, 1998).

[27]"A New Start for the Defense Industry," at http://info-france-usa.org/profil/glance/start2.htm

[28]*Ibid*.

[29]"France Advances on Infowar Front," *Intelligence Newsletter*, Volume 289 (June 6, 1996).

[30]Speech by NATO Secretary General, Dr. Javier Solana, "NATO: Its 50th Anniversary—The Washington Summit—The Next Century," January 25, 1999.

CHAPTER 23

THE RUSSIAN UNDERSTANDING OF INFORMATION OPERATIONS AND INFORMATION WARFARE

By
Timothy L. Thomas

Finding similarities in the Russian and U.S. approaches to information operations (IO) is not a difficult task. Both countries' specialists closely study electronic warfare and command and control systems of other countries, and both stress the importance of the use of computers and information management in the preparation and conduct of modern combat operations. This includes the use of information to conduct psychological operations (PSYOP).

Upon closer examination, however, the Russian approach to the information warfare (IW) aspect of IO has several elements that makes it unique and different. There are three principal reasons for the distinct Russian method.

First, there is the issue of overall context. The Russian state, economy, and society are in a transition period resulting in institutional and philosophical instability. Russian mass consciousness, according to many prominent scientists and government officials, is vulnerable to manipulation by slick marketing campaigns and to exploitation by promises of economic and social prosperity during this transition period. As a consequence, the Russian specialists' approach to information threats places strong emphasis on what it terms information-psychological processes as well as state laws to guarantee the information security of individuals and society.

A second reason for a dissimilarity in emphasis is that traditional Russian military thinking developed differently than in the West due to geographical considerations, varied military threats, the economic realities imposed by a different ideological background, and the emphasis placed on the study of military affairs as a science. The Russian study of the impact of the use of information weapons on military art will differ in emphasis from the Western assessment due to this prism through which these operations are viewed and measured, a reflection of the military's traditional thought process.

Finally, the Russian approach is unique due to the budgetary, technological, and infrastructure restraints under which information capabilities are developing. Regarding the infrastructure, it is simply insufficient to handle the onslaught of new technological improvements associated with the information age. The phone system in Russia, for example, is antiquated, with a limited number of trunk lines to handle the volume of calls in most cities. It will be difficult to adapt this system to a greater load caused by computers. Technologically, it will be years before fiber optic cables arrive in some locations, and only recently have computer companies begun the production of all Russian component computers. The inability to produce miniaturized components in a modern production facility has been the major drawback. Severe budgetary restraints curtail other efforts to bring change quickly to the country.

As a result, Russian scientists have initially spent more time on IO theory than in the West, with the latter focusing on practice over theory. It will take several years for Russia to catch up with the West in the technological area. But backwardness can be turned to an advantage when others pay for the trial and error of first generation technology, provided that there is some plateau at which you reach reasonable parity.

Russian specialists acknowledge this backwardness as a fact and try to work with it. Even though the introduction of information technologies has been ongoing since the late 1970s, it is only during the 1990s that up-to-date systems have been produced. In a discussion of the "information IQ" of the armed forces, that is the ratio of the quantity of equipment required to that in existence, 450,000 computers were noted as still needed, compared to only 25,000 presently in existence. This yields an IQ of 18 out of 100. At that rate, it will take 50-60 years to get to an IQ of 90. Russia probably will get to that figure much faster now that it is starting to mass-produce its own computers. The goal should be attainable in no more than 5 to 8 years, if the budget allows for it. It will be hard to divorce the military IQ from the societal IQ in this area.

In addition to these three reasons, it is also important to remember that only a handful of experts write openly about information operations in Russian military journals in contrast to the hundreds of authors who publish on the subject in the West. Since there is not an official Ministry of Defense [MOD] regulation or publication that defines and outlines the Russian concept of IW, the West must depend on the viewpoints offered by a few serving and retired officers, narrowing the scope of the dialogue. Fortunately, many of these officers are not only experts in the area but are responsible for teaching information operations subjects at academies and institutions in Russia. Their opinions are worthy of close consideration.

These factors should be considered in the discussion of ten key elements of the Russian approach to information warfare that follows. First, however, a short description is offered of the Russian view of the terms information security and information warfare that serve as a base for the remainder of the discussion. These terms are themselves unique in that they reflect both the Russian experience and dialectical thought process.

Defining Information Security

Russia's national security concept as well as several state laws refer to information security as a national interest of Russia. One of Russia's first attempts to develop a draft law on information security was in 1995. An equivalent document does not exist in America. In defense, this unique and comprehensive assessment discussed critical areas, the status of information security in Russia, perceived threats to information security, methods of providing information security to the state, and the organizational structure and principles of a system of information security. It listed critical areas as:

- information resources of the Ministry of Defense, General Staff, main staffs of the components of the armed forces, and scientific-research establishments; information, facts, and figures about the preparation and conduct of operational and strategic plans, deployments and mobilizations; and the tactical-technical character of equipment;

- information resources of the military-industrial complex as well as the industrial potential and quantity of raw materials available to the force; information on the basic direction of the development of the equipment of the armed forces;
- the country's command and control system of personnel and weaponry, and their information support;
- the political-moral condition of the force; and
- the information infrastructure (control points and connections, relay points, tropospheric and satellite communications), to include communications with other ministries.

External threat sources included:

- all types of intelligence activities;
- information-technical activities, such as electronic warfare and computer intrusion methods;
- psychological operations of probable enemies, either through special activities or through means of mass communication; and
- activities of foreign political or economic structures that work against Russia's interests in the defense sphere.

Internal threat sources included:

- disrupting established communication and information means in staffs and establishments of the Ministry of Defense;
- premeditated or unpremeditated mistakes of personnel in the information system of special significance; and
- information-propaganda activities of organizations and individuals directed against the interests of the government that result in the lowering of the prestige and combat preparedness of the armed forces.

The draft noted that these threats are particularly dangerous when the military-political situation is aggravated. The information security draft also divided the main methods for improving information security in the defense sphere into three areas:

- conceptual: structure goals to provide security in the defense sphere, i.e., goals which flow from practical tasks or missions, and a correct evaluation of information threats and their sources;
- technical: improve the means of protecting information resources from methods of unsanctioned access by developing protected, secure systems of command and control and raising the reliability of computer resources; and
- organizational: form the optimal structure and composition of functional organs of a system of information security in the defense sphere and coordinate their effective cooperation, improve the methods of strategic and operational disinformation, intelligence gathering, and electronic warfare, and improve the methods and

> means of actively counteracting information-propaganda and psychological operations of a probable enemy.

According to the best available information, this draft has not become law. However, a host of other laws (draft or otherwise), edicts, and statutes on information operations already exist.

Defining Information Warfare

While no official (that is, MOD, Security Council, or Defense Council approved) military definition of information warfare has been endorsed to date, several unofficial ones are available from speeches or articles. What makes them distinct is that they are careful not to copy the U.S. understanding of the term. Russian analyst V. I. Tsymbal has noted that "it makes no sense to copy just any IW concept. Into the IW concept of the MOD must be incorporated the constitutional requirements of the Russian Federation (RF), its basic laws, specifics of the present economic situation in the RF, and the missions of our Armed Forces." In addition, Tsymbal points out, in the RF the organs of state security are responsible for the accomplishment of IW in the broad definition of the term.

Partial confirmation of this fact was recently affirmed by the attempt of the Federal Agency for Government Communications and Information (FAPSI) to have the State Duma allow FAPSI to control the Internet in Russia. FAPSI, the former KGB Eighth Chief Directorate and Sixteenth Directorate, alleged that the CIA was creating information weapons and combat computer viruses, and FAPSI control over these attempts was needed.

Russian definitions of IW encountered thus far do seem to adhere to a common theme that differs from the U.S. view, namely that information warfare is conducted in both peacetime and wartime. In its peacetime use, the term refers to the information security of society and the government in the psychological, scientific, cultural, and production aspects, among others. In its wartime use, it refers to the attainment of superiority in the use of information protection and suppression systems, to include command and control, EW, and reconnaissance.

Retired Admiral Vladimir Pirumov is perhaps the most authoritative person to define the term so far. He is a former instructor of electronic warfare and now is the Scientific Advisor to the President of Russia. He defines information warfare as follows:

> *"Information warfare" is a new form of battle of two or more sides which consists of the goal-oriented use of special means and methods of influencing the enemy's information resource, and also of protecting one's own information resource, in order to achieve assigned goals. An information resource is understood to be information which is gathered and stored during the development of science, practical human activity and the operation of special organizations or devices for the collection, processing, and presentation of information saved magnetically or in any other form which assures its delivery in time and space to its consumers in order to solve scientific, manufacturing, or management tasks.*

His definition implies that information warfare is an activity that can be carried on in peacetime as well as wartime. For strict wartime scenarios, Pirumov offered a definition of information warfare in operations that aimed at gaining an information advantage:

> *"Information warfare in operations (combat actions)" is the aggregate of all the coordinated measures and actions of troops conducted according to a single plan in order to gain or maintain an information advantage over the enemy during the preparation or conduct of operations (combat actions). An information advantage assumes that one's own troop and weapon command and control components are informed to a greater degree than are those of the enemy, that they possess more complete, detailed, accurate, and timely information than does the enemy, and that the condition and capabilities of one's own command and control system make it possible to actualize this advantage in combat actions of troops (forces).*

Other Russian definitions of the term information warfare are also available. V.I. Tsymbal, a Ministry of Defense civilian analyst mentioned earlier, offered both a broad and narrow definition of information war, noting that:

> *In the broad sense, information warfare is one of the varieties of the "Cold War"—countermeasures between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people's public/social awareness, to state administrative systems, production control systems, scientific control,*

> *cultural control, etc. It is namely in this sense that the information security of the individual, society, and state is usually understood.*
>
> *In the narrow sense, information warfare is one of the varieties of military activity/operations/ actions (or the immediate preparation for them) and has as its goal the achievement of overwhelming superiority over the enemy in the form of efficiency, completeness, and reliability of information upon its receipt, treatment, and use, and the working out of effective administrative decisions and their purposeful implementation so as to achieve combat superiority (victory) on the basis of this. The waging of information warfare in the narrow sense is the field of responsibility of mainly the ministers of defense of modern states.*

A final definition is offered by Colonel S. A. Komov, a Candidate of Technical Sciences and Professor. He defines information warfare within the confines of an article that looked only at its wartime use, defining it as:

> *…a complex of information support, information counter-measures, and information defense measures, taken according to a single design and plan, and aimed at gaining and holding information superiority over an enemy while launching and conducting a military action/battle. Interconnections between information warfare and other types of operational/combat support and activities that make up its contents should be noted as well (intelligence, information gathering, communications, etc.).*

Komov believes four issues are at stake in his definition: first, identifying a set of measures to gain information on the opponent and on the condition of an engagement (electronic, weather, engineer, etc,), to gather information on friendly forces, and to process and exchange information between command and control echelons or sites; second, identifying measures to block the information gathering processes of others, and to feed deceptive information at all stages; third, identify friendly countermeasures; and finally, gain information superiority over the enemy.

Do these definitions compare favorably with the U.S. definition of information warfare? According to Department of Defense Directive S-3600.1, approved on 9 December 1996, IW is defined as “an information operation conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.” An information operation is defined as “actions taken to affect adversary information and information systems while defending one’s own information and information systems.”

Comparing the U.S. and Russian definitions, there are similarities and differences. One similarity is that both countries include the concept of defending one’s own information (in Pirumov’s definition, information resources) while affecting the information of an adversary. In addition to pure information, the U.S. definition includes information systems as items to be affected or defended. The Russian definitions are broader and encompass considerations of the information security of society in both peacetime and wartime, while the U.S. definition confines itself to time of crisis or conflict.

This short discourse demonstrates a concern as we talk about information operations: we are using two different languages and conceptual approaches in our attempts to define terms. The U.S., for example, does not define information resource or information advantage or a term used later, information potential. Russians, on the other hand, have trouble finding a precise Russian term for the concept of information warfare, using several names to describe it. These include information voyna (war), borba (struggle), and protivoborstvo (confrontation), with all taken to mean information warfare as well.

Ten Key Elements of the Russian Approach

In the past, some of the key elements that defined Russia’s approach to the study of military operations included officers’ interpretations of the principles of war (Russia’s 13 versus the U.S.’s 9); the nature of armed conflict; the coefficient of effectiveness of nuclear weapons; an evaluation of the military potential of a possible enemy; the correlation of forces of two opposing sides; and arms control concepts such as deterrence and parity, among other subjects.

The current study of military operations reflects many of these elements, but with an information operations twist. This was apparent in the concepts of information security and information warfare outlined above. While not direct parallels, one is able to discern that military thinking has adjusted and metamorphosed, resulting in terms such as “the development of information-psychological operations,” the “study of the computer-operator interface, the “effect of information operations on arms control issues such as parity,” the “scrutiny of the information potential of a country," the "effect of information operations on military art, especially the understanding of the initial period of war," the "use of computer viruses as weapons," the "development of neuron computers and the infosphere," and the "ability to use space and information based assets to detect and kill an enemy force with speed, precision, and stealth."

The first key element to the unique Russian approach to information warfare is what theorists refer to as "the natural laws and principles associated with information warfare." Komov ascertains that the identification of the objective laws and principles of IW are urgent problems for the development of the scientific theory of IW. Pirumov states that he has already done this, and notes that the general, universal laws and principles of armed battle remain fair and useable in the information battle. However, the information battle also has its own specific inherent aspects as well. Pirumov lists the law-governed patterns (trends and predictive in a mathematical sense) of the information battle as follows:

1. The constantly growing role of information warfare in carrying out assigned missions in the combat operations of troops (forces). This is determined primarily by the increased informatization of the armed forces and, consequently, by the increased means and forces which are enlisted for this informatization. It should be noted that the advent of new means and methods of information warfare does not carry with it a rejection of the traditional means, methods, and forms of armed battle, but it does have an impact on the methods of resolving combat missions with the help of traditional

means, and it also changes the capabilities of traditional means and the effectiveness of the combat use of troops (forces).

2. Information warfare today is carried out both in war time and in peacetime. In the latter instance, the means of information warfare are employed in order to diminish the enemy's information resource prior to the commencement of combat actions. It should be noted that the conduct and consequences of information warfare are not always known to the side against whom it is being conducted.

3. The ever growing impact of informatization on all levels and spheres of governmental and military control systems provide some basis for identifying information warfare as an independent form of armed battle. The reason for this is that most developed nations today possess powerful information potential which under certain conditions can be concentrated and utilized to achieve their own political goals. Two factors lend added appeal to such an approach in resolving external political conflicts, i.e., the current trend of avoiding the use of armed force in international conflicts, and the lack of international legal norms which would regulate the methods of conducting information warfare.

The basic principles involved in organizing and conducting information warfare operations (combat actions) include, according to Pirumov:

1. subordinating the goals, missions and measures of information warfare to the missions of the troops in combat actions, as well as assuring that the information operations are so organized as to fit the plan and intent of the operation (combat actions);

2. preemptory resolution of the tasks of information warfare vis-à-vis the combat missions of the troops in combat actions;

3. a multi-purpose use of the forces and means of information warfare in the preparation and conduct of combat actions, as well as a rational combination of the measures of information warfare with the actions of troops to destroy the enemy;

4. the constant and covert conduct of information warfare throughout the entire operation (combat action); and

5. the principle of a counter system, according to which the forces and means enlisted for the conduct of information warfare must be unified into a functional system which is in no way inferior to the enemy's command and control systems.

Of course, the laws and principles examined here are not immutable. Rather, they are clarified as the content, forms and methods of conducting information warfare evolve or develop.

A second difference is the main objectives and methods of implementing information warfare concepts. This is a major difference due to the differentiation in peacetime and wartime missions.

In peacetime, IW is conducted secretly through means of intelligence, politics, and psychological actions, according to Pirumov. Actions are conducted against armed forces, the civilian population, and the systems for administering production, research, and culture. Each side seeks to undermine the information security of the individual, society, and the state of the opposing side, while safeguarding one's own information security. The main role here is played by government propaganda institutions, foreign intelligence, and counterintelligence, as well as institutions protecting information. Most important is the fact that an ever increasing role is played by specially programmed hardware and software techniques against the information assets of the engineering systems of the enemy, that is, virus warfare.

In wartime, Pirumov says, IW operations are more overt. They act as a system supporting the traditional forms and methods of warfare. They also support information and intelligence activities, and the secrecy of primary activities of friendly troops in the preparation and conduct of operations. They assist with measures for obtaining surprise (especially in a period of threat such as the initial period of a war) and can drastically reduce the information assets of the forces and diminish their combat possibilities, while protecting one's own forces if jam-proof equipment can be developed. The primary way to do this is to disrupt enemy command and control systems and weapons, while protecting these systems on the Russian side.

The main methods or means by which one can engage military information systems, Pirumov continues are:

1. physical destruction or taking actions to prevent an operation, such as capture of operating personnel or other actions by assault groups or special detachments, fire strikes on the systems, actions of reconnaissance groups, or incapacitating the systems;
2. electronic countermeasures against designated command posts and electronic facilities;
3. the use of specially programmed hardware and software techniques against information assets of automated control systems, or for the surprise destruction or blockage of information assets of potentially dangerous states at the start of combat actions;
4. distortion of information used by the enemy to evaluate a developing operational-strategic situation or for decision-making (PSYOP or manipulation effect); and
5. psychological impact of IW operations on leaders and servicemen of the facilities of systems of command and control.

The main forms of IW and electronic warfare, IW's main component, Pirumov posits, are:

1. a special operation to disrupt enemy command and control;
2. EW attacks;

3. an information blockade (for example, through the use of an electronic blockade); and
4. the systematic actions of forces and assets utilized in IW functions.

There are three levels at which IW is conducted, according to Pirumov:

1. state;
2. scientific and technological; and
3. weapons systems and technology.

At the state level, the aim of IW is to lower the information potential of probable enemies while supporting the information security of the state. At the scientific and technological level, the aim is technological superiority to ensure parity or superiority in military power due to advanced information and technological assets. These assets must be able to withstand the electronic impact or counteractions of the enemy while protecting one's own assets. At the level of weapons systems and technology the goal is to conduct actions against sources of information threats to eliminate, suppress, or reduce their effectiveness. Measures must also be taken to protect ones own command and control elements.

A third and perhaps primary difference in the Russian and Western approach is the Russian focus on the impact of information on members of its society. This "information-psychological" aspect of information warfare is not as predominant in the U.S., where electronic warfare, defensive and offensive mechanisms, and digitalization of the force/information dominance are the centers of interest. American society is relatively stable and, at least for the present, the impact of foreign influence on the U.S. mind and psyche is viewed as minimized By contrast, the Russian emphasis is understandable since society lost its cementing mechanism, the ideology of communism, when the USSR disintegrated. Only control over the "information-psychological" aspect can produce the mental stability the country desperately needs to allow it to proceed with future reforms and to rebut rumors and disinformation, in the view of many sociologists and scientists.

Russian candidate for President and Communist Party Chief Gennadiy Zuganov, who believed he was a victim of an information-psychological strike by the Yeltsin campaign during the Presidential elections of June and July 1996, underscored the importance of information for Russian society in a recent interview:

> *It is necessary to remove the quotation marks from the concept of "the fourth estate" and to legally recognize state electronic mass media as an autonomous—information—branch of power besides the legislative, executive, and judicial branches.*

Zuganov's emphasis corresponds to the traditional importance placed on the moral-psychological factor by the Russian military, since the moral-psychological factor is regarded as one of the 13 principles of war.

Fourth, and closely associated to the information-psychological element, is a serious attempt by the Russians to harness the energy generated by human beings. The so-called "Computer Operator's Security Problem" is a multi-disciplinary one, these scientists believe, connected to the integrative efforts of different areas of knowledge—physics, biology, psychology, cybernetics, philosophy, and religion. From this perspective, if man is viewed as an open system capable of communicating with the environment using material, energy, and information flows, then it is possible to influence him by means of radiation (electromagnetic, acoustic, etc.) and to cause changes in the psycho-physiological condition of his organism. In addition to energy sources, information alone can also influence the vital processes of a person if it is properly packaged. This theory appears to have strong appeal for such Russian scientists as Victor Solntsev and Vladimir Pirumov, who often write on information operations.

Solntsev, for example, believes that to all people the world appears as diverse forms of information flows, which everyone processes differently. Certain forms of radiation-information fields, according to these scientists, can cause disease, disorder of the gums and systems of an organism, modification of behavior, suppression of thinking, manipulation of one's consciousness, and the destruction of one's personality, among other problems. Deaths have resulted in Russia from the computer-operator interface as well, they report:

> *August 13, 1994. There was an accident in Voronezh City. One user of a personal computer lost consciousness in less than 20 minutes. His friend—a programmer—said that he had a strange feeling, as though…he had a headache and some noise in his ears. It was almost impossible to stop it, as though it was some type of hypnoses. Luckily he managed to shut off the computer. His friend was dead some time later,*

> *never regaining consciousness. The diagnosis was bleeding inside the brain.*
>
> *The cause of his death was a computer virus named "666." Experts determined that it produces on the computer monitor a so-called 25th frame with a special color combination, that can immerse the person in a sort of hypnotic trance. Each 25th frame the picture changes. And the subconscious perception of the new pattern results in arrhythmia of the heart. Blood pressure sharply increases, and then falls sharply. And blood-vessels of a brain cannot withstand these pulses. Later, nearly 50 similar cases of sudden death were registered.*

To date, the Russians have not talked openly about their use of computer-generated morphed images, but they have referred on more than one occasion to the U.S. use of holographs in the operations in Somalia and during Desert Storm. In addition, the priorities of the Committee on Science and Technology indicate that research is underway in this area. Most significant in the Committee's list was the reference to speech, text, and image recognition and synthesis systems under study, as well as artificial intelligence and virtual reality systems. Some Russian scientists believe that technical objects, the consciousness of a person, and the group consciousness of a community can be affected through the computer-operator interface. Others are studying the perception-machine operator interface.

Fifth, Russia views information operations developments as phenomena that have not only tactical and operational but geo-strategic significance. Superiority in information technologies, as an example, could debilitate a nuclear coding or launch command procedure. This would make the more traditional "numbers and megatonage" norms of parity disappear as information technologies become capable of disabling these systems and causing them to be either unreliable or unusable. Information warfare systems (including intelligence and information collection) do this by upsetting existing nuclear and conventional norms of parity based primarily on numbers and quality, the Russians believe. Intelligence, command and control, early warning, communications, electronic warfare, "special software engineering effects," and disinformation are issues that contribute to superiority on the battlefield in ways different than before and upset the traditional correlation of forces. They can also be used as a hidden form of military-political pressure. In this sense, Russia considers information operations to be a key geo-strategic element capable of upsetting the status quo. Information operations, for example, can bring catastrophic results in a number of areas—an information strike on a strategic command and control site can relinquish control over assets, an information strike at a national power grid can lead to a destruction of hardware, or an information strike at the control systems of a nuclear power plant can lead to a melt down. None are excluded from warfighting or even peace-time covert information strikes.

Sixth, Russia calculates the information potential of a country as a measure of that country's military power that is information based. Components of information potential lie in essentially two areas. The first is information resources, defined by Pirumov as information which is gathered and stored during the development of science, practical human activity, and the operation of special organizations or devices for the collection, processing, and presentation of information saved magnetically or in any other form which assures its delivery in time and space to its consumers in order to solve scientific, manufacturing, or management tasks. The second is information means, those assets that carry out tasks in the launching and conduct of an operation.

Another category is the information potential of a weapon, which is the degree to which a weapon is "informationalized," that is, the degree to which a weapon's internal components rely on information or computer functions to attain maximum effectiveness. There is an additional linkage between economic-societal potential and state and then military information potential.

Seventh, information operations greatly affect the study of military art, in the view of some Russian military specialists. They view these operations as a separate and self-sufficient type of conflict; as operations that make the initial period of war extremely uncertain (one doesn't know what preparations were or are being prepared by a potential opponent during peacetime to alter the effectiveness of weapons or the strategic perception of the situation at hand, implying that the initial period of war may already have started); and as operations that increase the tempo of battle, focusing on continuous attacks designed to blind an opponent by destroying his information operations capabilities and achieving information dominance.

If the form of warfare is changing under the influence of informatization or computerization, then there will be changes in military art as well. Pirumov, for one, believes that there are three ways that military art is being effected. First, the rapid development of communications facilities along with the appearance of various automated control systems and increased numbers of combat assets now enable unity and coordination of combat actions on heterogeneous forces and their fire interaction without spatial concentration (allowing for new operational ideas such as the air-land nature of combat actions). Second, computerization allowed us to see deep through reconnaissance-in-depth equipment and facilities, increasing the accuracy of destroying enemy facilities. Thus, the concept "second-echelon combat" offers opportunities to deliver precision selective strikes against enemy reserves moving up, on his rear facilities, and so on. Finally, operations will no longer be conducted cyclically, with intensive operations followed by lulls. Rather they will be conducted continuously, making it important to kill an enemy immediately after he is detected. This means warfare will evolve to "detect-kill" and a "reconnaissance-strike-jam" concept will be inevitable. Decisive superiority will be gained by the side having command and control in real time, demanding a new level of computerization in the armed forces.[25] Winning the battle of the ether is winning the battle.

In Tsymbal's view, the conduct of IW is felt at all three levels of military art: strategic, operational, and tactical. He noted that in peacetime, the goal will be to accumulate information on an enemy while developing and testing one's own IW weapons. Immediately prior to military action and during military action, IW systems will work to destroy first of all command and control systems of the enemy and any other information systems which receive, store, or process information of military significance. Or, an IW operation will be run independently prior to the onset of combat actions of the traditional type.[26]

Perhaps the most important targets identified through a study of military art are those battlefield systems that work in tandem to first uncover and then destroy an object, the reconnaissance-strike and reconnaissance-weapon complexes. There is a need to have real time and accurate battle-damage assessment for this to really work and counter any "maskirovka" or deception attempts. Asked to demonstrate the relation of processes that lead detection to kill mathematically, one Russian scientist offered the following:

> *destruction capability equals exposure of an object (via satellite or reconnaissance asset) times asset's precision and speed of its components*

All of these assets (reconnaissance, acquisition, control, precision, etc.) are interconnected and controlled by the infosphere (see key element 10) if the latter is understood to be programs for processing, storing, and creating data. The satellite locates, the precision guided weapon uses data sent by the satellite, and the information component of the weapon determines Ks speed and accuracy.

Acquiring and fixing the force in a manner compatible with this line of reasoning is a priority and one of several areas of agreement between Russian and Western thinking. Even a cursory look at Russian military writings underscores the importance placed on the acquisition of the location of the enemy by a military force, followed by fixing the enemy force through fire. As one analyst noted:

> *The increase in fire capabilities of the troops, the appearance of high-precision weapons, and the development of various types of guided missiles are objectively increasing the role of reconnaissance and command and control systems. In conditions when the likelihood of hitting targets with the first shot or salvo is approaching 1, reaction speed is becoming a paramount factor. The main targets of battlefield reconnaissance are enemy artillery and armored equipment.*[27]

Target detection as a result is now of primary importance to the Russian military. The pages of the Russian military journal *Military Thought* carried a serious discussion of no fewer than seven articles from 1994 to 1996 that discussed effective target engagement (ETE), that is, how to acquire and destroy enemy targets. The discussion was thorough, covering such aspects as should ETE be zonal or target (area or point) oriented, how can it be integrated into combined arms criteria of successful combat action, and so on. One article noted that productive ETE “mainly depends on how quickly information flows from reconnaissance agencies are transformed into command and control impacts on ETE assets,” among other items. This is a random process, however, and only a certain degree of probability can be expected.[28] This emphasis on acquisition also coincides with changes predicted by Pirumov on changes in military art.

General Colonel N. M. Dimidyuk, Commander in Chief of the Missile Forces and Artillery of the Ground Forces, concluded the ETE discussion in *Military Thought*. He called for closer integration of assets, noting that "under present conditions ETE cannot be separated from the EW [electronic warfare] suppression of enemy command and control, information, and reconnaissance systems and networks.[29] This led to the emergence of ETE as "one decisive factor determining the course and outcome of a combat operation and often times of a war as a whole…,[30] and to the use of ETE assets to "disrupt enemy troops and weapon command and control systems at the very start of an operation, to inflict a decisive defeat on the main enemy forces and logistical installations, and to seize and maintain fire superiority"[31] through coordinated and massed use while attaining surprise. Such coordination will require that:

> *the main task…is coordination of the ETE plan with the operation's objective, concept, and design, which can be achieved only in the event that ETE planning is carried out by an operational (combined-arms) staff command and control agency: the ETE planning and coordination group (ETE PCG)…This will shift the center of gravity in ETE planning to the operational level…*[32]

Dimidyuk concluded by noting that:

> *the results of the discussion show that in assessing ETE, it is appropriate to use a single indicator that has a graphic physical interpretation and is easily integrated into the operational criterion used in operation planning: the force incapacitation rate expectation. It should objectively reflect strike, reconnaissance, maneuvering, and other capabilities of the forces*

> *in question that characterize their striking power in an offensive and their operational stability in defense. It needs to be finally recognized that not enough has been done yet in substantiating the requisite correlation of the sides' forces in operations of various types and scale, when the combat capabilities of the forces are expressed through their combat potentials.*
>
> *…with respect to same-type (homogeneous) multiple targets, the ETE rate affecting the target's combat capability is defined by the number (proportion) of individual targets to be engaged, whereas with respect to different-type (heterogenous) targets, it is defined by their composition (combination). While there can be several such combinations, it is believed that if at least one target out of this combination is not effectively engaged, then it retains its combat capability and is therefore in a condition to perform its functions.*[33]

Eighth, the computer research and development process has produced some unexpected results unique to the Russian experience. One is the neuron computer, expected to replace the pentium chip for speed and effectiveness. Other areas identified and approved by the government's Science and Technology Committee as priority directions for federal-level technologies in information related fields included multiprocessor parallel-structure computers; computer systems based on neuronet computers, transputers, and optical computers; speech, text, and image recognition and synthesis systems; artificial intelligence and virtual reality systems; information and telecommunication systems; mathematical modeling systems; microsystem technology and microsensors; superlarge integrated circuits and nanoclectronics; optical and acoustic electronics; cryoelectronics production technologies; laser technologies; precision and mechatronic technologies; robotic systems and micromachines; electronic-ion-plasma technologies; intellectual systems for automated design and control.[34]

Of particular interest in this list are the neurocomputers. According to one report, these computers are now being developed in Russia. They are reportedly 1,000 times faster than traditional computers, according to Yuriy Glybin, deputy head of the State Committee for Defense Industry. Military uses include the development of state-of-the-art high-precision weapons, military equipment, optic devices to detect missiles, as well as use in ABM programs and dual technologies. In financial markets, the computers are used to make highly accurate forecasts (supposed 90 percent accuracy) of currency and futures rates, stocks. and other securities.[35]

Ninth, Russian scientists, recognizing the increased importance of systems, have focused more attention on the interaction of combat systems instead of on simple force on force (the old correlation of forces) ratios. This approach differs from the U.S. systems approach by its dialectical nature, measuring combat systems against one another instead of in isolation. According to this logic, warfare is viewed as the interaction among the military systems of the sides in confrontation. This idea has extended to modeling at the General Staff Academy, where Red versus Blue force-on-force reportedly is no longer played as it once was. Instead, high tech systems are modeled against other high tech systems.[36] Integrating these systems is also important, as other analysts have noted:

> *…the reconnaissance-information-command and control component ensures system integrity. Therefore, as a rule it also acts as an object of information confrontation; its disorganization, neutralization, or destruction leads to the disruption of system integrity and to a loss of its potential capabilities.*[37]

Within the discipline of military systemology, information is viewed as the “nourishment” that gives life to all elements of the system from top to bottom, according to one expert. This applies in particular to reconnaissance, conmmand and control, support, and strike systems. Information warfare as a system, according to this view, includes three components: information support of the functioning of one’s own combat systems: information counteraction against the functioning of the enemy’s combat systems; and information protection or defense of one’s own combat systems against the informational counteraction of a possible enemy.[38]

In short, the side that cannot conduct real-time fire control on an enemy force is doomed to defeat in large scale conflict, and in some conflicts of lesser intensity as well. Emphasis is on the ability to acquire and process information through systems utilizing space or the airways, and resulting in target acquisition:

> *The number of information sources for tactical command and control systems is growing. Use of remotely piloted reconnaissance vehicles*

> *[RPVs] is becoming more and more widespread. Radar detection and command and control aircraft…are being improved. All this leads to a growing interconnection and interdependence of air and ground weapons. The airways are becoming a distinctive "fourth dimension" of the space in which combat is waged. Fighting is also waged in them: radars and communications equipment are jammed, radiation sources are discovered and destroyed, and electro-optical surveillance systems are blinded.*[39]

Finally, one of the most important factors considered from a technical standpoint is that "the infosphere, understood as a body of general and specialized programs for creating, processing, and storing computerized data, is bound to become one of the most likely objects of military conErontation."[40] Specifically, Russian scientists are worried about the impact of hostile actions to influence the infosphere through such items as "algorithm bombs" capable of distorting a section of an algorithm that limits the ability of software to function as required and "software bombs," those bombs that insert an uncalled for algorithm that limits the execution of software functions or that steers it to commit computations unauthorized by the software program as originally intended. This final key factor is also a major element of the U.S. approach to IW.

This idea first was described in an article from 1991 by Russian Captain Vladimirov, who noted that:

> *In the French air defense systems sold to Iraq, so-called "logic bombs" were installed, which*

> *made it impossible to use these systems against the multinational force during combat operations in the Persian Gulf. An American missile went off course and was blown up on command from the ground, because a "1" instead of a "7" was indicated in its computer program…[Thus] the effectiveness of electronic computers depends upon the quality of the software. Defects in the form of incorrectly written sections of programs frequently result in a complete breakdown of the systems…Sabotage bugs substantially exacerbate the problem of quality and reliability of software.*[42]

Since software programs run many systems, it is no surprise that Russia has developed viruses to affect these systems. Four types of computer viruses were listed by one Russian analyst, although it was unclear if he was referring to Russian or U.S. variants of these viruses.[43] The Russians also claim to have developed a "stealth virus."[44] This virus does not allow for its detection by the usual method, comparing file space with total free space, and so is termed stealth. By the year 2000, Russian scientists also expect to confront "distance virus weapons," computer viruses introduced through radio channels or laser lines of communications directly into computers that pose an instant threat to command and control means of units such as the strategic missile force.[45] A final threat is the use of "microwave weapons," electromagnetic impulses designed for use against the electrical components of Russia's space, aviation, ground, and sea-based means of combating information warfare.[46] Russia is also studying how to develop and implement these means, according to some sources.

The infosphere can become a target of hostile intentions in peacetime or wartime, according to Russian analysts. Attacks are most dangerous if aimed against the target acquisition systems and command and control setups of a nation.

Conclusions

The 10 elements outlined above highlight some of the terminology and conceptual landmarks that outline Russian thinking on the problem. Are these elements really different from the Western approach?

Clearly, identifying the targets of information operations for any country is easy: EW systems, command and control nodes, satellites, and AWAC planes stand out as clearly today as targets as did massive armored formations 50 years ago. What is really different is the conceptual understanding of an information operation from a cultural, ideological, historical, scientific, and philosophical viewpoint. Different prisms of logic may offer totally different conclusions about an information operation's intent, purpose, lethality, or encroachment on sovereignty; and this logic may result in new methods to attack targets in entirely non-traditional and creative ways.

Russia's approach is a reflection of its dialectical logic, the historical processes that have shaped it, and its efforts to adjust to a new environment. In the past, control over information was dominant. Even Xerox machines were off limits to many people. Today, Russia is battling a creeping "information anarchy" that, in the opinion of its citizens, is saturating society. Citizens are confused over just what to believe when they are reading the papers or watching television. The problem is just as difficult for the military. Threat perceptions were developed over the course of many years. While there is a reason and cause for cooperation with the West, the military must engage in these discussions with a wary eye. They still tend to blame the end of the Cold War on a successful information operation run by the West that destroyed not only the Soviet Union but communism, the country's unifying ideology. Why would the West not engage in another ambitious undertaking to further its control over Russia, the military asks.

The primary concern is that in its attempt to catch up with the West in information operations, Russia does not appear to have a clear idea where it will end up when the process is finished. This is reflected in the military definition of terms such as information warfare which are much more vague, open to interpretation, and a cause for misunderstanding than in the past. What do Russians mean when they refer to an action as an "information-psychological" strike? What are the ramifications of such an action? Will it be an accusation of a violation of international law or will it result in a nuclear exchange? Where are the areas of misunderstanding on the U.S. side that can cause a similar response?

Much remains to be done to overcome the terminological and conceptual problems associated with unique parochial views of information operations if we are to avoid information confrontation or warfare in the future. The 10 elements listed in this paper are important considerations that, in a general fashion, represent a unique and different way of looking at the problem. As the U.S. and other nations continue to cooperate with

Russia, everyone should pay close attention to one another's thinking in this sensitive area. Conflict prevention or crisis management techniques are needed here every bit as much as they were over nuclear weapon concerns in the past. Further, a comparative analysis of Chinese, U.S., Russian, Canadian, German, and British views, among others, is required to understand the extent of this problem, not to mention to help avoid both current and future problems in the area of information operations.

[1] For example, Russian specialists put a physiological-psychological spin on Pavlov's reflexive control, while Westerners saw it as a biological process.

[2] Alexander Yegorov (interview with Victor Bazhenov), "Kaz izmenit' 'voyennyy intellekt" ("How to change the 'Military Intellect"), *Krasnaya zvezda*, August 3, 1996, p. 5.

[3] Dmitriy Semenovich Chereshkin and V.A. Virkovskiy, "Kontseptsiya informatsionnoye bezopasnosti Rossiyskoye Federatsii" (proekt) ("The Concept of Information Security of the Russian Federation") (draft), Moscow, 1994.

[4] *Ibid*., p. 19, 20.

[5] *Ibid*., p. 20.

[6] *Ibid*., pp. 20-21.

[7] *Ibid*., p. 21.

[8] *Ibid*., p. 21.

[9] These Laws, edicts and statutes include the following: Draft: "Concept of information Security of the Russian Federation," 1994; Law: "Federal Law on Communications," passed by the State Duma on January 20, 1995; Edict No. 65: "On the Ratification of the Statute on the Russian Federation Presidential Staff's Information Administration;" Law: "Russian Federation 'Federal Law on Information, Inforrmatization, and the Protection of Information," enacted by the State Duma on January 25, 1995; Directive: "On the Confirmation of Lists of Informations, Relation to State Security," November 30, 1995; Edict: "Edict of the President of the Russian Federation, "Measures to Regulate the Development, Production, Sale and Purchase for Purposes of Selling, Importing into, or Exporting out of the Russian Federation, as well as the use of Special Technical Equipment Intended for Secretly Obtaining Information," January 1996: Statute: "Statute

on the Council of Heads of State Information Agencies of the Commonwealth of Independent States," February 1996; Directive: "On the Development of a Situation Centre within the Federal Government Communications and Information Agency (FAPSI)," April 1996; Decree: "On a Special Comprehensive Program for Creating Communications, Television, and Radio Broadcasting Technologies," May 1996; Law: "On Participation in International Information Exchanges," July 1996.

[10] Professor V.I. Tsymbal, "Kontseptsiya 'informatsionnoy voyny' ("Concept of Information War"), paper received at conference with the Russian Academy of Civil Service in Moscow, September 14, 1995, p. 2.

[11] Russia Reform Monitor, No. 215, January 10, 1997, American Foreign Policy Council, "Former KGB Reportedly Tries to Control Internet in Russia."

[12] From a speech delivered in Brussels in May 1996 by Admiral Pirumov, "Certain Aspects of Information Warfare," p. 2.

[13] *Ibid*.

[14] Tsymbal, pp. 3-6.

[15] S.A. Komov, "Information Warfare in Modem War: Theoretical Problems," *Military Thought*, May-June 1996, pp. 76-70.

[16] Pirumov, pp. 3, 4. The laws and principles in the text are taken from these pages of Pirumov's report.

[17] *Ibid*., p.9.

[18] *Ibid*., pp. 9, 12, 13. The writeup on the wartime use of IW as well as the methods and forms of IW is a summary of the main points of these three pages of Pirumov's text.

[19] Pirumov, p. 5.

[20] Gennadiy Zyuganov, "On the Threshold of a 'Government of Seven Boyars'," *Sovetskaya Rossiya*, October 26, 1996, pp. 1, 2.

[21] Victor 1. Solntsev, "Information War and Some Aspects of Computer Operator's Defense," paper presented at the InfoWarCon 5, Washington D.C., September 4-6, 1996, pp. 2-7.

[22] *Ibid*., p. 7.

[23] "New Trends in Power Deterrence," *Armeyski Sbornik*, No. 9 (September 1995), pp 12-19, as reported in FBIS-UMA-96-011-S, January 17, 1996, p. 12.

[24] I. Panarin, Georgi Smolyan, Vitaly Tsgichko, and Dmitriy Chreshkin, "A Weapon that may be more Dangerous than a Nuclear Weapon: The Realities of Information Warfare," "*Nezavisimoye Voyennoye Obozreniye* (supplement to *Nezavisimaya Gazeta*), November 17, 1995, No. 3, pp. 1-2, as reported in FBIS-UMA-95-234-s, December 6, 1995.

[25] Pirumov, pp. 14, 15.

[26] Tsymbal, p. 11, 12.

[27] Sergey Grigoryev, “Who Will Fire First? The Eyes, Ears, and Nervous System of the Ground Troops,” *Nezavisimiaya Gazeta*, August 22, 1996, No. 16 (20), p. 6.

[28] V. Ye. Shulgin and Yu. N. Fesenko, “Effective Target Engagement Planning in Combined-Arms Operations,” *Military Thought*, (January-February 1996), pp. 33, 34.

[29] N. M. Dimidyuk, “Principles of Effective Target Engagement: Summing Up the Discussion,” *Military Thought*, (May-June 1996), p. 16.

[30] *Ibid*., p. 15.

[31] *Ibid*.

[32] *Ibid*., p. 16. Dimidyuk added three pages later that “the importance of the group’s coordinating role grows especially in implementing the zonal-target principle of ETE planning. It is called upon to ensure, above all, an efficient coordination of fire delivery with ETE assets under the control of the superior commander in the area of responsibilty of subordinate levels: and coordination of actions by ETE and EW assets of the air force, missile forces, artillery, air defense forces, and special troops, and in maritime sectors those of battle front forces, in delivering massed and concentrated strikes. The need for coordinating the ETE plan with the operation’s overall objective and concept highlights the necessity to relate the indicators characterizing the expected ETE results with the results of the operation as a whole. Furthermore, it is key to provide for the possibility of ensuring the integration of the ETE indicator (measure) into the operational criterion used in elaborating the concept and objectives of an operation, and in decision-making. Considering that this indicator is the correlation of the sides’ forces, calculated through the combat capabilities of their contingents, one indicator of the effectiveness of the engagement of enemy forces, as a number of authors pointed out during the discussion, can be the extent to which their (the forces’) combat potentials are reduced—a measure that in the present situation is assumed as their combat incapacitation rate expectation.”

[33] *Ibid*., pp. 20, 21.

[34] Andrey Fonotov, “Science and Technology Policy,” *Rossiyskaya Gazetta*, August 8, 1996, p. 6, from FBIS-UST-96-037, August 8, 1996.

[35] INTERFAX, February 14, 1996. as reported in FBIS-UMA-96-040-S, February 27, 1996, p. 64.

[36] Based on a discussion with modelers at the General Staff Academy in December 1991, during a visit by a Fort Leavenworth Command and General Staff delegation.

[37] Nikolay Turko, Sergy Modestov, and Nikolay Shvets, “…And Data Confrontation,” *Armeyskiy Sbornik*, October 1996, No. 10, pp. 92, 93.

[38] Author's discussion with General-Major (retired) V. D. Riabchuk, Fort Leavenworth, September 1996.

[39] Grigoryev.

[40] A.N. Kukashkin and A.I. Yefimov, "The Security of the Infosphere of Strategic Defense Systems," *Military Thought*, No. 5, 1995, pp. 45-48.

[41] *Ibid*., p. 46.

[42] A. Vladimirov, "Informatsionnoe Oruzhie: Mif ili Rea'lnost'?" ("Information Weapons: Myth or Reality?"), *Krasnaya Zvezda*, October 5, 1991, p. 3.

[43] Aleksandr Pozdnyakov, "Informatsionaya Bezopasnost" ("Information Security"), *Granitsa Rossii* (September 1995), No. 33, pp. 6-7; as reported in FBIS-UMA-95-239-S, December 13, 1995, pp. 41-44. These viruses are: 1) trojan horse virus, which is introduced into the victim system, remains idle for a certain period of time, and then causes catastrophic destruction of the system; 2) forced quarantine virus, which is introduced into a network and knocks out the program of the unit into which it was planted. If components are not separated, then the entire system network is destroyed; 3) overload virus, which quickly spreads throughout the entire system and gradually slows its operation; and 4) sensor virus, which penetrates a preplanned sector of a computer's data storage area and, at a critical moment, destroys the data bank and its information.

[44] Pal'chun, B.P., and R.M. Yusupov, "Obespecheniye Bezopasnosti Komp'yuternoy Infosfery" ("Providing Security in the Computer Infosphere"), *Vooruzheniye, Politika, Konversiya*, No. 3, 1993, p 23.

[45] M. Boytsov, "Informatsionnaya Voyna" ("Information Warfare"), *Morskoy Sbornik*, No. 10, 1995, pp. 69-73.

[46] *Ibid*.

CHAPTER 24

INFORMATION-BASED WARFARE AND THE PRC

By
M. Ehsan Ahrari

In essence, information warfare is political warfare.

—From "PRC: Dialogue on Information Age, State Security," (Chinese) *National Defense University Journal*

As many articles in the first volume of *The Information Age Anthology* intimated, the information revolution is permeating all walks of life in industrialized countries. Who would have thought that in a little more than a century after the industrial revolution the world would shrink into a true "global village?" One cannot even say that the information revolution is the culmination of industrial revolution-related human progress. In many respects, it appears to be just another phase of a string of scientific and technological progress that is continuing.

The United States is far and away the lead country in the realm of the information revolution. Indeed, even with the end of the Cold War, the United States has continued its research and development endeavors with a view to maintaining its supremacy in information technologies.

Many (but not all) of the research and development efforts in information technologies are now driven by private industry rather than federal funding. In some respects, this reflects the "declinist" school within the United States that gained prevalence in the 1980s and early 1990s about a possible decline of the United States. Even before the Cold War ended, Paul Kennedy's suggestion that great powers must not waste their economic capabilities to maintain their military power was taken to heart by American leaders.[1] As a result, defense spending declined.

Even so, the United States' leadership in the realm of information technologies and capabilities was especially noticed by the world during the Gulf War of 1991. Lessons from the Vietnam imbroglio were learned extremely well. The military was not committed until the nation was behind the U.S. involvement in the Persian Gulf. The United States had a very clear sense of its military objectives in that conflict. As important, politicians stayed out of the warfighting business.

Even though all wars are fought and won on the basis of information dominance, the Gulf War of 1991 was portrayed as the "first information war." What was special about this war was that information technology played a very crucial role. The decisive dominance of the high-tech-based U.S.-led coalition only contrasted with an equally high level of chaos and "blindness" experienced by the Iraqi armed forces.

Military establishments all over the world watched the performance of the U.S. armed forces during the Gulf War with a mixture of envy and awe. While it has been said that military establishments in general continue to fight the last war, one can extend this aphorism and state that a major conflict is fought again and again not only by the military forces that were directly involved in the conflict, but by all military forces. Thus, other military forces use the Persian Gulf War in developing their future battle plans and in conducting their wargames.

This is particularly true about the Gulf War of 1991. The performance of the U.S. armed forces, based on high-tech capabilities, is being studied, incorporated, and practiced by the military forces of all the industrial countries, especially by potential competitors and adversaries of the United States. Even several developing countries are becoming more and more interested and knowledgeable on information warfare-related issues. While neither developed nor developing states can presently emulate the American performance in the Persian Gulf given their respective resources and levels of technological sophistication, they nevertheless intend to learn from it, and perhaps improve their own capabilities in the future.

The focus of this essay is the PRC. Emerging as an industrial giant, China has enjoyed an average growth rate of 10 percent since economic reforms were implemented there in 1978. It has the world's second largest foreign currency reserves at $105 billion reported in January 1997, a foreign trade surplus of $124 billion, and a total foreign investment of $42 billion in 1996.[2] It is also spending a large amount of its resources on enhancing its capabilities in information-based warfare.

Even though the trade ties between Washington and Beijing are sizable, the PRC has done little to conceal its strategic interests, some of which may conflict with those of the U.S. and therefore raise the level of tension between the two countries in coming years. Since Beijing perceives the U.S. presence in Southeast Asia as an essential aspect of Washington's attempts at building a containment coalition against China, the latter has been involved in attempts at counter-containment. One may envision the Sino-Russian strategic partnership as an added wrinkle of the Sino-American strategic maneuvering. Even though ongoing strategic maneuvers and counter-maneuvers are generally benign, they might not remain so in the future. China's views on Taiwan and its human rights policies have remained two of the major sources of contention between Beijing and Washington.

More to the point, China is determined to emerge as a dominant power in the Asia Pacific. Given the fact that an "established American objective" in the Asia Pacific is to prevent "any single country from gaining overwhelming power in Asia,"[3] one cannot rule out the possibility of a future military clash between the Unitred States and China.

Chinese Perspectives on Information Warfare Dynamics

Given the Chinese military leadership's fascination with the U.S. conduct of the Gulf War, there is little doubt that in the next conflict, the PRC is likely to employ its own version of information-based warfighting techniques. Just how strongly has the PRC's military establishment been persuaded about the lethality of information warfare techniques that were so effectively used by the U.S.-led coalition during the 1991 Gulf War?

Lt Gen Huai Guomo's depiction of how to fight an information war, though written in 1996, is a good general description of the techniques used by the U.S. military in the Gulf War. He writes:

> *Before a battle begins (sometimes dozens of hours in advance) and proceeds, commanders will first use offensive information-war means (precision guided weapons, electronic jamming, electromagnetic pulse weapons, and computer viruses) to attack enemy information systems, affecting or destroying their decision-making mechanisms and procedures, thus forcing an end to the fighting in line with the aspirations and terms of the offensive sides. And meanwhile, to protect their own information and information systems from enemy destruction, they will set up in combat space among all targets and weapons real-time detectors—links among shooters. Such offensive-defensive information warfare will become the focus of coming wars. The struggle for information supremacy will gradually become the crux of the battle, in a sense as strategic deterrent.*[4]

If further evidence is needed of the "nature of lessons learned" from the Gulf War by the Chinese military leaders, one only needs to consider the following observation made by Jen Jui-Wen:

> *China has realized from the outcome of the Gulf War several years ago that unlike the human wave tactics of the agricultural age and the iron and steel warfare of the industrial age, air raids and precision strikes from long distances are decisive factors in the outcome of wars. It also*

> *realizes that information warfare and electronic warfare are of key importance, while fighting on the ground can only serve to exploit the victory.*[5]

One of the most significant influences of the Gulf War on the thinking of the Chinese military analysts is their conclusion that "People's War Under Modern Conditions" has undergone an irreversible change. Since the Gulf War of 1991, they believe, soldiers equipped with low technology like the soldiers of Iraq and the PRC will encounter a decisive tactical disadvantage when faced with high technology-equipped American (and to a lesser extent, other Western) soldiers. Consequently, many Chinese authorities assert that new information technologies are particularly important in local wars.

The Chinese military establishment is therefore preoccupied with emerging as a high technology force in the 21st century. An examination of the writings of its military analysts underscores the fact that they are avid readers of American professional military journals and the futurists, whose work has also deeply influenced the thinking of senior American military leaders.

While Chinese defense studies closely follow the thematic changes in warfighting doctrines and their implications for the warfighting capabilities of the U.S. military, it is not clear whether Chinese defense specialists have paid much attention to the debate over the military technological revolution (MTR) in the American military profession and its nuanced changed focus on the revolution in military affairs (RMA). Nor is it clear whether the Chinese have taken any position on the U.S. debate. Chinese scholars tend to use the terms MTR and RMA interchangeably. It is possible that for the PRC military establishment, the distinction between the two means little. However, the Chinese remain keen on the American military's commitment to the notion of jointness in warfighting, its heavy reliance on precision weapons, high resolution imagery, and satellite technology, and its emphasis on interoperability of weapons.

One scholar, Su Enze, believes that the MTR has already happened. "Guided and represented by information warfare," he writes, "a military revolution is also taking place in military ideology, military theory, military establishment, combat pattern, and other military fields on a global scale."[6] The author notes a distinction between "technical" and "technological" revolutions. The former is defined as "revolution of military skills and military techniques," whereas the latter, according to him, means "scientific, academic, and systematic developments in military fields."[7] Su Enze notes that electronic warfare (EW) precedes information warfare. As he envisions it, EW originated from radar technology (i.e., tuning and jamming technology), telecommunications (which was employed in the command, control, and intelligence fields), and finally developed into C3I and precision guided weapons.

An interesting aspect of this essay is Su Enze's observation that information warfare is "shrouded in strange circles." The first circle, according to him, is that "the information source should be situated in an area where information is most needed. However, we need information to locate such an area." Elaborating, the author notes that in the absence of the Soviet Union, the United States is looking for a "new primary target." The second circle is that "the further technology develops, the more easily technology will be caught up with." He implies that this might be good news for Third World countries that are looking for technological short cuts. The third circle is that "the further information technology develops, the more fungible and vulnerable information technology becomes." The fourth strange circle, according to the author, is that computer-based electronic or network war is "the first stage of intelligence warfare whereas a strategic war is a higher and more brilliant stage of war."[8] Su Enze concludes with the observation that the 1991 Gulf War, like previous wars, was "machinery warfare" despite success in the use of information-related technologies. He implies that this reality should be kept in mind, especially by Third World atates seeking information warfare technologies and capabilities.

PRC scholars are quite sensitive to the notions of information as a prime strategic source in warfare and of the importance of intelligence in contemporary warfare. One author writes:

> *In strengthening the information concept as a multiplier of commanders, we must take information as a multiplier of combat effectiveness and see it as a strategic resource more important than men, materials, and finances, so that it can be properly gathered, employed in planning, and utilized. We must make efforts to raise our capacity to obtain, transmit, utilize, and obstruct warfare information and must include these elements in the whole process of command training.*[9]

In addition to keeping close track of technical writing, research, and development by their professional counterparts in the United States, PRC defense analysts and the military establishment also study information warfare-related developments in Europe.[10] As in the United States, the military in the PRC has served as a main source of research and development. For instance, Cai Renzhao writes that Chinese military industries converted over 3,000 technologies to civilian use. In facing the “stern challenges” of the Information Age, he emphasizes, “military and civilian cooperation and tapping the military potential of the ‘information superhighway’ are major measures we must adopt.”[11] Chinese defense specialists, like their American counterparts, are searching for the “perfect weapon” in information (digitalized) warfare. One hears the echo of Admiral William Owens’ advocacy for “the system of systems.”[12] Cai Renzhao recommends that the PRC “should try to gain insight into the development situations of foreign military forces, try to understand future warfare, accurately recognize the differences between ourselves and foreign military forces, fully bring our own superiority into play, and explore the ‘perfect weapon’ on a digitalized battlefield.”[13] He recommends that the PRC follow the European Union’s example in a “focused way” and learn lessons from the United States and Europe in developing information-related research. “The PRC,” according to Cai Renzhao, should “fully bring into play the guiding role of information warfare research in building the military.” It should also, he says, “seek measures by which to launch vital strikes in future warfare, so as to damage the enemy’s intelligence gathering and transmission abilities, and weaken the enemy’s information warfare capacity.”[14]

InfoWar and the Military as a Warfighting "Network"

Conventional organizations in the Information Age are undergoing major changes. The notion of hierarchy is becoming outmoded. In its place multi-organizational networks are emerging. The U.S. military has performed a trail-blazing task of undergoing radical changes in response to the radically divergent techniques of warfighting in the Information Age. It is called "joint warfighting," but it serves as an umbrella phrase under which a multitude of changes are taking place.

This is not a place to enumerate those changes. Suffice it to say that under the auspices of the Goldwater-Nichols Act of 1986, the U.S. military has not only been busy converting the task of joint warfighting into an art form, but is continuing to do more with less. This means that the U.S. military is continuing to come up with different organizational and functional (i.e., tactical) ways to serve as a credible warfighting force. In fact, *Joint Vision 2010* has emerged as an abbreviated discussion of the utmost significance assigned by the military to information warfare.

Chinese defense analysts also are at the cutting edge of studying the implications of information war for traditional institutions like the military. Xu Chuangjie writes, "The revolution in information technology has increasingly changed with each passing day the battleground structure, operational modes, and concepts of time and space while dealing blows to the traditional 'centralized' and 'tier-by-tier' command structure." He cites the U.S. Army's example of building a "ground force operational command system," which is an attempt "to organize various command control systems of the…ground forces into an integrated mutually linked network to realize 'shared information' from the national command authorities on top down to a grass-roots unit."[15] He emphasizes the significance of strengthening, completing, and perfecting the building of the C3I command system for the PRC. He also recommends that: a) the C3I command system "at and above the battalion level of various services and service arms" be turned into an integrated mutually linked network; b) the traditional vertical and tiered command system be converted into a network command structure in order to meet the demands of time and flexibility in command; and c) the centralized type command system should gradually be developed into a dispersed command system.[16]

In an apparent reference to netwar and cyberwar, another Chinese military analyst, Wei Jincheng, writing in *Military Forum*, observes, "The technological revolution only provides a stage for confrontation. Only when this revolution is married with military operations can it take on the characteristics of confrontation." Underscoring the multidimensionality of information warfare, he writes, "The rapid development of [computer] networks has turned each automated system into a potential target of invasion. The fact that information technology is increasingly relevant to people's lives determines that those who take part in information war are not all soldiers and that anybody who understands computers may become a 'fighter' on the network." He goes on to note, "The multi-dimensional, interconnected networks on the ground, in the air (or outer space), and under water, as well as terminals, modems, and software are not only instruments, but also weapons."[17]

Elaborating on the impact of the military technical revolution on future war, Lt Gen Huai Guomo touches on networks as follows:

> *In the C4I system, the traditional command system at the vertical level will be reduced, while lateral links will be increased, with the tree (or trunk) command system changed to a network form. That will help to increase command flexibility, bringing the initiative and creativity of commanders at all levels into full play, raising the capability and effectiveness of coordinated operations, and improving survival capability.*[18]

The Chinese defense establishment has been quite conscious of its country's vulnerability to potential acts of sabotage during peacetime, as well as potential attacks during a military conflict, and is taking steps to reduce this vulnerability. Wei Jincheng writes, "An information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from an enemy."[19] Discussing the use of viruses in a netwar or even a cyberwar, another defense scholar writes, "Computer viruses can be used to track down enemy's target system and the enemy's guided missiles may end up attacking the side which has launched them or deviate far from the intended target….After locating its target, a virus may replicate rapidly, erasing the normal operating database, thus overwhelming and crippling the computer system." The same article discusses the variety of measures taken by the U.S. military in reducing its vulnerability to potential attacks, including sabotage attempts from terrorists and hackers.[20]

The military establishment in the PRC is watching the recent research on and development of "virus warfare" in the West with rapt attention. The main focus of its interest, once again, is the U.S. military. One essay notes with interest a news item in the *Philadelphia Inquirer* that the U.S. military has developed a computer virus that can destroy an enemy's computer circuits and control systems, "transmit internally information that mistakenly reports enemy's orders, and distort the computer satellite software that the enemy transmits to his combat units." The same essay discusses another "computer virus weapons plan" that the U.S. armed forces are in the process of developing. This program reportedly is aimed at planting viruses in exported computers and electrical equipment. The "virus source" implanted in such equipment can be activated during the time of military conflict, causing the enemy's electronic equipment to malfunction.

This essay concludes with a number of suggested preventive measures against future netwar or cyberwar. First, it advocates raising the consciousness of military computer security in the China's armed forces. Second, it asks the PRC military establishment to pay special attention to removing "hidden perils to hardware and software security," by creating security filters and careful tests on all imported electronic equipment. Finally, it recommends the initiation of "special-topic research on computer viruses."[21]

The Future

As one ponders the future of U.S.-PRC relations in the context of information-based warfare, three observations come to mind.

First, even though the Chinese military establishment wishes to emerge as a high tech-based warfighting machine, its present state of preparedness poses absolutely no threat to the United States armed forces. In fact, it is safe to say that in the conventional warfare, the United States military, purely on the basis of its commitment to practicing its professional trade, the state of its readiness, and the sophistication of its equipment and logistical infrastructure, is unbeatable. Only Russian nuclear weapons—and to a lesser extent, Chinese nuclear weapons—pose a credible threat to the United States in a future military conflict.

Second, this reality should not let anyone forget the current commitment of the Chinese armed forces to high-tech warfare. If continued with zeal, this is likely to pose a serious challenge for the U.S. in the coming years. The state of readiness of the Chinese armed forces in the realm of information-based warfare in the early 21st century may be at a very primitive level compared to the U.S. armed forces. Martin Libicki is of the view that "Militaries—especially those of widely different nations—cannot prosper by copying each other." He adds, "Their endowments, circumstances, and strategies differ greatly. Each must adapt the general to the specific. We know the Chinese can copy our thoughts, but whether they can innovate in pursuit of their own objectives is not yet obvious."[22] My own sense is that the Chinese have proven themselves remarkable in adapting Marxism to indigenous requirements to suit their own cultural needs. Similarly, they are likely to develop information-based warfare techniques to suit their special needs before too long. The United States must remain specially sensitive to this profound historical reality about the PRC.

Third, China's smaller neighbors must not only watch the Chinese military preparedness closely, especially in the realm of information-based warfare, but also try not to remain too far behind in this field. This is not to suggest that the PRC and its neighbors are likely to fight one or more wars in the near or distant future. Rather, it is to suggest that the military establishments of a number of countries of East Asia are being equipped with state-of-the-art weaponry, and they are well-served to emulate the U.S. military preparedness in the realm of information warfare-related technologies as much as possible.

[1] Paul Kennedy, *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500-2000* (New York, NY: Random House, 1987).

[2] International Institute for Strategic Studies, Strategic Survey 1996-97 (London: IISS, 1997), pp. 162-63, passim.

[3] Richard Bernstein and Ross H. Munro, "The Coming Conflict with America," Foreign Affairs (March-April 1997), pp. 18-32.

[4] Huai Guomo, "On Meeting the Challenge of the New Military Revolution," as translated in *Foreign Broadcast Information Survey-CHI*, Number 130, 1996, pp. 1-7. (Hereafter *FBIS-CHI*.)

[5] Jen Jui-Wen, "Latest Trends in China's Military Revolution," as translated in *FBIS-CHI*, Number 047, 1996, pp. 1-4.

[6] Su Enze, "Logical Concepts of Information Warfare," as translated in *FBIS-CHI*, Number 135, 1996, pp. 1-5.

[7] *Ibid.*, p. 2.

[8] *Ibid.*, pp. 4-5.

[9] Lei Zhoumin, "Information Warfare and Training of Skilled Commanders," as translated in *FBIS-CHI*, Number 036, 1996, pp. 1-5. Also consider the following description of war in the Information Age:

> *Ordinarily, the enemy precedes a firepower bombardment with an electronic bombardment in order to wipe out our command structure, paralyze communications, blind radar, and render weapons ineffective. Then, after soft killing and wounding by electronic bombardment, large numbers of guided weapons conduct hard killing and wounding to wipe out our combat strength. Therefore, without a very good*

> *electromagnetic defense capability, and without a quick reaction early warning communications system, an extremely great price will have to be paid when war occurs suddenly. Otherwise, opportunity and capability to make an effective counterstrike may be lost.*

This passage is from Zhang Xiaojun, "Modern National Defense Needs Modern Signal Troops," as translated in *FBIS-CHI*, Number 100, 1996, pp. 1-5.

[10] Chinese military specialists are also undoubtedly keeping close track of other military-related developments and may also be engaged in espionage in their attempts to acquire state-of-the-art technology both in the United States and in Western Europe. China's close collaboration with Israel may also be one of the ways the PRC obtains top-of-the-line Western defense technology through legitimate business deals.

[11] Cai Renzhao, "Exploring Ways to Defeat the Enemy through Information," as translated in *FBIS-CHI*, Number 100, 1996, pp. 1-5.

[12] For Admiral Owens classic article on the "system of systems," see *U.S. Naval Institute Proceedings* (May 1995), pp. 35-39.

[13] Renzhao, *op. cit.*, pp. 4-5.

[14] *Ibid*., p. 4.

[15] Xu Chuangjie, "Military Revolution Gives Impetus to Evolution in Command," as translated in *FBIS-CHI*, Number 030, 1996, p. 1.

[16] *Ibid*., pp. 1-2.

[17] Wei Jincheng, "New Form of People's War, as translated in *FBIS-CHI*, Number 159, 1996, pp. 1-3.

[18] Huai Guomo, *op. cit.*, p. 5.

[19] Wei Jincheng, *op. cit.*, p. 3.

[20] Zhou Li and Bai Lihong, "Information Warfare Poses Problems," as translated in *FBIS-CHI*, Number 014, 1996, pp. 1-2.

[21] Chou Hsi, "Exploration and Analysis of Military Computer Security and Virus Protection," as translated in *FBIS-CHI*, Number 116, 1996, pp. 1-6.

[22] Personal exchange by the author.

CHAPTER 25

THE THIRD MILITARY REVOLUTION

By
Ch’en Huan

- Up to the present, there have been three military revolutions: Before the 1930s, the large number of units equipped with airplanes, tanks, and radios touched off the first military revolution, proclaiming that mankind had passed from the era of “cold weapons” into the era of “hot weapons.”

- From World War II to the 1960s, the development of nuclear technology and the use of guided missile technology on the battlefield brought about the second military revolution, proclaiming the arrival of the “nuclear-hot weapon” era, followed by the development of nuclear strategy and the theory of nuclear deterrence.

- Following the rapid development of information technology, stealth technology, and long-range precision strike technology, the Gulf War, which occurred at the beginning of the 1990s, opened the curtain on the information war era and marked the sudden appearance of the third military revolution.

Without the slightest doubt, like all previous military revolutions, the third will have far-reaching effects on military practice and theory.

The Challenge to Traditional Operational Principles

Concentration of military force is an operational principle universally followed by strategists in ancient and modern times, in China and abroad; it is mainly achieved by increasing the density of unit-space military force. Following the rapid development of technology and its increasingly widespread application in military affairs, the ancient military principle of concentration of military force must be reconsidered and viewed from a new angle:

- First, from a look at the object of concentration, we see that military force concentration in the traditional sense is no longer effective; it has been replaced by the concentration of striking efficacy, including firepower, electromagnetic energy, photo energy, information energy, and other energy forms. Because of the development of information technology and its widespread application in weapons and equipment, all the methods of information warfare create conditions, under modern circumstances, that allow concentration of combat-effective energy without needing to concentrate large units. Provided these weapons are deployed in a dispersed manner, they can attain the operational objective; deployment in a concentrated manner, on the contrary, leads to trouble.

- Second, from a look at the component parts of concentration, we see that the position and role of “software” is constantly rising. Armed force “software” (including the level of intelligence of officers and men, the level of armed force control of information energy, and other invisible factors) is gradually occupying the dominant position in warfare and its role is becoming larger day by day.

- Third, regarding the methods of concentration, a “soft” strike force is even more important than a “hard” strike force. If we liken military force and weapons to a “hard” strike force, then electronic countermeasures and other information war measures are a “soft” strike force. The application of high technology makes electronic and information technologies widely permeate all weapons and equipment, all operational measures, and battlefield commands, so that information warfare technology permeates every important measure in the operational domain and runs through the entire course of a war, directly influencing the course and outcome of the war.

From a look at the object of concentration, we see that striking the other side’s effective force is no longer the main starting point, and the focus is now on interfering with and destroying the other side’s information and cognitive systems. By striking at one point one can achieve the operational objective of paralyzing the entire body. “Destroy the enemy and preserve oneself” is another operational maxim that all armed forces, in ancient and modern times, in China and abroad, have always followed. However, in warfare in the information era the tendency is for military forces to be deployed in a dispersed manner, the demarcation line between the front and the rear to disappear, and weapon systems to reach over the horizon and cross national boundaries.

The method of the past in which a decisive battle with the enemy's main force was sought makes it difficult to grasp the opportunity for battle and also makes it difficult to achieve ideal results. However, provided the enemy's information system and his command and decisionmaking system are destroyed, countered, or interfered with, thereby destroying his capability to obtain, process, transmit, control, and use information, we can paralyze the enemy's entire operational system and thus he will lose his operational capability. This has more results in actual combat than continually killing or wounding many troops, and continually destroying many ordinary weapons. That is to say, the meaning in the traditional sense of "destroy the enemy and preserve oneself" should be extended to "strike the enemy's information system and ensure our side's capability for information warfare."

From Physical to Cerebrum Countermeasures

In the "cold weapons" era, armed forces mainly depended on the physical ability to use weapons when waging war, and their overall combat effectiveness was only the multiplication of the individual combat effectiveness of their soldiers. Even in the "hot weapons" and "hot-nuclear weapons" eras, armed forces were skilled armed forces; among operational units there existed a relationship of a clear division of work and coordination; the overall combat effectiveness was the square of the sum of the collective combat effectiveness. In armed forces with information weapons, rank-and-file soldiers, who originally depended on their physical skill in using mechanized weapons and equipment, will be replaced by specialized software that mainly depends on intelligence in using weapons and equipment that has been transformed by information. This “multiplier” effect of intelligence and information almost leads to a limitless expansion of the combat effectiveness of conventional weapons and equipment.

In a certain sense, for armed forces in the information era the test of strength is between intelligence capabilities, and the core of the third military revolution is the development and use of information capability. Therefore, some people say: If we say that in the two previous military revolutions, because of the use of chemical, thermal, and nuclear energy, man’s physical capability was extended and man’s four limbs were liberated, then the third military revolution, which develops and uses information capability, will extend man’s intelligence capability and liberate man’s cerebrum. The armed forces of the future will be “high-tech forces” with photoelectric specialists, information specialists, aviation specialists, and other outstanding specialized talents as its core.

Lines Between Front and Rear Will Blur

In a future war there will be nonlinear attacks on enemy objectives. The concepts in the “hot weapon” era of a battle front and an operational depth will lose meaning. The main reasons for this are:

- First, all kinds of information-transformed platforms and information-transformed weapons have sprung up like bamboo shoots after a spring rain; operational capability has reached the global level, and five-dimensional operations—air, land, sea, space, and electromagnetic—have become the main operational forces in high-tech warfare. Battle lines of the past, like the “Maginot Line” and the “Bar-Lev Line” are no longer terrifying shields, and they are also not chasms that cannot be crossed. The conventional one-by-one breakthrough tactic of first going to the forward position and afterward to the in-depth position is no longer effective. The operational sequence could be going first to the in-depth position and afterward to the forward position, and the objects of strikes could be first the support and technical units and afterward the combat units. The way to achieve victory is not necessarily occupation but rather the destruction by firepower of information capability. The disappearance of the battle line causes the front and the rear to lose their support conditions dependent on differentiation.

- Second, the operational objectives of the two sides on attack and defense are neither the seizing of territory nor the killing of so many enemies, but rather the paralyzing of the other side’s information system and the destruction of the other side’s will to resist. The enemy’s command centers, communication hubs, information-processing centers, high-tech weapon control systems, and supply systems could become priority targets of attack. The scenes in the past of close-combat fighting have become history, and where the front and the rear are located is no longer an issue of concern to commanders and units.

Rapid Rise of New Operational Concepts

The vigorous development of information-transformed weapons will make fundamental changes in the traditional operational concepts, thereby causing many new operational forms to appear in future wars.

Long-Range Combat

Previously, because the performance of weapons and equipment was limited, quite a few strategists were fond of the tactic of "close combat." Now, there has been a great increase in the types of long-range antipersonnel methods. Among them, the air arm, the over-the-horizon precision strike force, and the large amount of equipment of electromagnetic units will replace the face-to-face ground attack units of the past and become the main strike forces in future operations. The further development of long-range strike weapons will make long-range combat an operational form in future wars. There will be three main forms of long-range strikes in the future: the first form is the one in which the air arm independently carries out long-range strikes; the second form is one in which the long-range strike combines with the long-range rapid movement of troops transported by land and sea with the vertical airdrops of airborne forces; and the third form is five-dimensional—air, land, sea, space, and electromagnetic—long-range combat.

Outer Space Combat

Under the impetus of information technology and other high and new technologies, satellites, space shuttles, manned spaceships, and space stations have appeared in succession. The following new-concept weapons will come forth in a continuous stream—all these weapons will make outer space the fifth dimension operational space following land, sea, air, and electromagnetism:

- Laser weapons
- Ultra- high frequency weapons
- Ultrasonic wave weapons
- Stealth weapons
- Mirror-beam weapons
- Electromagnetic guns
- Plasma weapons
- Ecological weapons
- Smart weapons
- Logic weapons
- Sonic weapons

Because the efficacy of these new-concept weapons depends on the hard-shell support of a space platform, once the space platform is lost their efficacy will be weakened and they will even become powerless. In this way the two sides in a war will focus on offensive and defensive operations conducted from space platforms in outer space, and these operations will certainly become a new form in future wars. In the U.S. Armed Forces a new service—the Space Force—is being discussed, showing that the idea of outer space combat is close to moving from theory to actual combat.

Paralysis Combat

This tactic does not make the elimination of the enemy's effective forces its objective, but rather takes as its starting point the destruction of the enemy's overall structure for combined arms operations and the weakening of the enemy's overall efficacy in combined arms operations. Under high-tech conditions, all subsystems of combined arms operations are mutually replenishing and inseparable operational groups. If there is no unified command and control monitoring and early warning by the information-transformed C^{3}I system, then it is difficult to obtain timely, reliable intelligence. Additionally, when there is an assault it is also impossible for the subsystems to coordinate without electromagnetic superiority, assaulting units become "blind persons," and even if they have more troops and weapons than the enemy they are nothing but a pile of trash. Therefore, by striking at the "vital point" of the enemy's information and support systems one can at one blow paralyze the enemy and collapse his morale.

- *Computer Combat:* The computer has infused powerful vitality into modern military machines, but it also has unavoidably been reduced to an object of attack. Once a computer system is damaged so that it cannot operate normally, cruise missiles and other precision-guided weapons become arrows without targets; and high-tech performance aircraft, tanks, warships, radar, and activated command systems will be totally in the dark about what to do. Engaging in computer combat can be compared to borrowing on the battlefield the principle of "Sun's understanding that boring a hole in the Iron Fan Princess's belly causes internal damage." Relevant data show that, before. the outbreak of the Gulf War, American intelligence organizations put a virus into Iraq's air defense system, which led to the destruction of 86 percent of the Iraqi forces' strategic targets in the first 1 or 2 days of the war. This also shows that making the computer an operational means of attacking the object of a strike has already become a reality. One by one, many armed forces have now put an enormous amount of funds into research on the types, methods, and results of computer virus invasions and attacks, and they have come up with all sorts of ideas, e.g., concealing a "virus source" in the integrated circuits of enemy computers and, when necessary, activating the virus by electronic measures, propagating, and duplicating it. Again, for example, with the aid of electromagnetic waves, a virus can be injected from a long distance into the enemy's command and communication systems and into the computers on his aircraft, tanks, and other weapons, causing "nonlethal destruction."

- *Radiation Combat:* In wars of the past, the power to inflict casualties mainly depended on the effects of kinetic energy and thermal energy, but the weapon systems produced by the third military revolution mainly use sound, electromagnetism, radiation, and other destructive mechanisms. Operational actions in which armed forces use radiation-damaging energy to strike at the enemy's electronic equipment, weapon systems, military equipment and personnel, and other military targets are called "radiation combat." The main radiation weapons are laser weapons, microwave weapons, particle beam weapons, and subsonic wave weapons; they possess enormous military potential.

- *Robot Combat:* The latest advances in information technology, artificial intelligence, virtual reality, and computer control have already provided the necessary conditions for developing functional robots. The main type of military robot on active service or about to be put on active service in the armed forces of various countries of the world are vehicle emergency robots, mine-laying robots, minesweeping robots, reconnaissance robots, transportation robots, electronic robots, and driver robots. Later there will appear engineer robots, chemical defense robots, patrol robots, and even unmanned intelligent tanks, unmanned intelligent aircraft, and other "robot soldiers." In essence, a robot soldier is an unmanned antipersonnel firepower carrier that possesses a certain capability for obtaining and processing information. It can complete many operational missions with a high degree of efficiency, and it can also avoid unnecessary casualties to the effective strength. In view of its strong points, there could appear armed forces with intelligent robot officers and men in primary roles. Once two belligerents put them on the battlefield at the most dangerous places and the most critical times, and they charge into battle, like the tank combat and missile combat before them, and similar to the robot wars in science fiction films, they will mount the stage of war.

"Thin and Flat" Command Systems

The armed forces command system in the "hot weapons" and "hot-nuclear weapons" era was a horizontally unconnected "tree-shaped" structure, which from top to bottom was in line with the units' in the military arm and branch establishments. This structure was convenient for centralized command, but it had a fatal weak point—its survivability was poor. If a branch of a tree-shaped structure is cut, that branch is affected, but if its trunk is cut, the entire structure is paralyzed. When the information-weapon era arrived, because of the large amount of use of the computer and the great improvement in its capability for searching, processing, transmitting, and displaying information, the various command and control systems could form an integral, mutually connected network connecting in one body the state's command authorities to the individual soldier, all of them sharing information.

Formation of the mutually connected system allows a front-line commander to directly obtain intelligence from general headquarters or space information centers, and the middle-level commander loses the reason for his existence. This will make the command system of future armed forces, because of the reduction in the number of levels, a thin and flat structure that is wide horizontally and short vertically. Therefore, this kind of command system is called a "thin and flat" command system. Its main characteristics are: all the network's nodal points are connected vertically and horizontally, thereby both maintaining the strong point of the past vertical connection between the upper and lower level units, which is convenient for centralized command, and have the capability to make direct connections between parallel units which is convenient for dispersed command. The "thin and flat" command system will lead to a change in the form of command, which will shift from the former centralized dispersed command, and, under a unified plan, the lower level commanders will have a primary role in decisionmaking. This thin and flat command system will be able to reduce the amount of information flow, shorten the line of information flow, ensure that the lower-level commanders obtain real-time battlefield intelligence, improve the capability for decisionmaking response, and fully display subjective capability.

Operational Simulation Will Play a Major Role

Modern operational simulation uses an especially large amount of computer operational simulation, applying it to simulate tanks, battle vehicles, artillery, surface ships, submarines, and many other weapons. It will also apply to different levels of strategy, campaigns, and tactics, thereby providing a scientific basis for decisionmaking.

Operational simulation—this "laboratory" for war—no matter whether in the domains of military science, armed forces system and establishment, weapon development, and military training, or in the aspects of selection of long-range delivery of military force and firepower, force composition, plan formulation, logistics and technical support, and tactical application, is playing an increasingly important role. For example, in unit training, by providing an operational simulation system that is sufficiently scientific and rational for tanks, armored vehicles, portable weapons, aircraft, helicopters, ground combat units, and other systems, training costs can be reduced, thereby greatly improving the beneficial results of training and increasing its safety. As of now, the U.S. Armed Forces have set up six laboratories for simulation techniques and methods. These six laboratories, by putting all arms and branches of the service on line with computers, can combine in one form the units, weapons and equipment with simulation equipment, and if necessary can conduct large-scale combined arms exercises. Britain, Russia, Japan, France, Sweden, and Israel are vigorously exploring the use of laboratories similar to those mentioned above.

“Smaller and Divisible” Structures

Following the development of information technology, any armed force will certainly tend to become smaller. At present the group army and division level scale structure widely used by the armed forces of various countries could become obsolete and be replaced by crack, intelligence-type small units that possess the capability for a high degree of mobility. In future operations, the attacking and defending sides will put more emphasis on being economical in the use of their operational strength, only throwing into the operations the essential units. A prominent characteristic of this kind of establishment is that it possesses “divisibility,” i.e., based on the nature and need of an operational mission, units can at will be “divided” and combined.

CONCLUSION

THE FUTURE OF DEFENSE POLICY:

INFORMATION AGE TRENDS

By
Daniel S. Papp and David S. Alberts

As the 21st century opens, we are only in the dawn of the Information Age. The first volume of *Information Age Anthology* explored the implications of advanced information and communication technologies and the capabilities they provide for broadly based human affairs. The second volume explored the implications of these technologies for national security. In this volume, we examined the Information Age's implications for war and the militaries that fight them.

As the preceding chapters have shown, there is much food for thought. Despite the wide differences of opinion and the uncertainty, eight trends seem to emerge. Some will be obvious, while others may be less clear.

Inevitably, these trends will drive a transformation of defense policy. The challenges associated with this transformation are formidable. America's best minds must give them their full attention.

We conclude this last volume in our series with the following eight observations or take-aways.

Information Age Technologies Will Be Ubiquitous, Immensely Enhancing Military Capabilities

Across the spectrum of military capabilities, from the tactical through the operational to the strategic, new and emerging Information Age technologies will provide military forces with capabilities that dwarf previous technological advances and innovations and, unlike previous advances, actually change the nature of war.

Intelligence, surveillance, and reconnaissance (ISR) capabilities will improve, allowing us to obtain far better information. Command, control, communications, computers, and information dissemination (C4I) capabilities will expand allowing us to share and collaborate more efficiently. Precision force (PF) applications will improve and grow allowing us to be more lethal and more discriminating. Information systems that enhance information access, management, and analysis in vital combat support areas will be further deployed providing us with a powerful set of new tools. Strategic information warfare capabilities will become standard elements in the U.S. military arsenal.

This is not to say that *Joint Vision 2010*'s operational concepts of dominant maneuver, precision engagement, full-dimensional protection, and focused logistics will be fully achieved any time soon. Nor will full spectrum dominance of all potential battlespaces be obtained. Technological, cognitive, and organizational challenges will remain. Opponents and potential opponents will develop countervailing capabilities and counter-measures, particularly asymmetric responses. And sufficient funds will never be available to acquire all the capabilities that the military deems necessary.

Nevertheless, advances in bandwidth, reliability, redundancy, and transparency will enable U.S. and allied military forces of the future to undertake actions that never before were possible. Increased bandwidth will expand information flows among friendly forces. Improved reliability will enhance connectivity even under highly stressful conditions. Greater redundancy will lessen the potential for system degradation and move the military toward more networked operations. Greater transparency will heighten confidence in the accuracy of information and the quality of decisions at all levels.

For the U.S. military—and for any other state or non-state actors that have the technological prowess, the funding, and the intention to take advantage of ubiquitous information and communication technologies—there will indeed be a revolution in military affairs. What to this point has been labeled a revolution in military affairs is truly limited in comparison to what is to come.[2]

The Sources and Types of Challenges and Threats to National Security Will Proliferate

For the U.S. military, the preceding paragraphs contain both good and bad news. The good news is that the

American military will be at the forefront of the expanding revolution in military affairs. It will be the first to take advantage of most elements of the revolution, and it will take advantage of the capabilities afforded by the revolution most fully.

The bad news is that the U.S. armed forces will not experience this revolution alone. Other international actors will also employ Information Age technologies, sometimes against U.S. interests. Thus, both the sources and types of challenges and threats to U.S. national security will proliferate in the Information Age.[3] This was discussed in detail in Volume II of the *Information Age Anthology* and pointed out again in Chapter 1 of this volume, but it is of enough significance that it bears repeating yet again.

Challenges and threats to U.S. interests will emanate from a variety of sources across the threat spectrum. At the high end, this includes state actors and terrorist organizations. In the mid-range, corporate espionage and organized crime present real dangers. At the low end, civil disobedience and politicized hacking may or may not be true challenges or threats. U.S. interests that may be challenged or threatened range from critical infrastructures such as energy, banking and finance, transportation, human services, and telecommunications to other vital American concerns such as military capabilities, business interests, and civil liberties.

The wide range of sources and types of challenges and threats raises questions about how U.S. national security should be defined in the Information Age. It also raises questions about how, whether, and when the government should initiate responses to challenges and threats once they are defined and identified. Which challenges and threats are truly challenges and threats to national security? Which endanger corporate security but not national security? Which endanger both corporate security and national security, and how should the distinction between the two be made? Which challenges and threats are more criminal activities than national security dangers? Which are unsavory or contradict social mores, but are not threats to security? Which may be disliked by authorities because of what they say and because of how they complicate government tasks, but are in fact genuine exercises of freedom of speech, assembly, or other civil and constitutional rights? Which are actions undertaken as a lark, but which nevertheless challenge or threaten national interests?

These are difficult questions to answer. Nevertheless, U.S. military and civil authorities—and the military and civil authorities of other countries as well—must grapple with them and develop widely accepted approaches that protect national security without undermining the foundations upon which democratic societies are based. At the same time, even as answers are being developed, the dangers posed by more traditional challenges and threats to national security must be countered. Given these conditions, the challenges of answering the questions posed above and of framing policy responses based on those answers are as difficult as meeting the technological and military challenges and threats that accompany the Information Age.

The Flow of Information About Battlespace Events Will Not Be Restricted to Militarily-Approved Sources

Despite news media complaints that the Department of Defense dominated, controlled, and manipulated information flow in military operations throughout the 1990s,[4] one of the most significant changes for defense policy in the Information Age will be the end of the government's ability to control and dominate information flows during times of war, conflict, and crisis. The combination of new on-the-scene communication and broadcast technologies and the increased access of non-governmental actors to space-based observation capabilities assures that points of view, broadcast images, and analyses of situations different from those presented by the government will make their way into the public domain and be widely available. This is true especially in democracies, but even in states with authoritarian regimes, alternative views will sometimes compete with official views for public attention.

In this respect, *Operation Desert Storm*, in which the U.S. government had significant control of information flows from the battle area, may have been the last Industrial Age war rather than the first Information Age war. Since *Operation Desert Storm* in 1991, and even since *Operation Noble Anvil* against Serbia in 1999, newer and more capable information and communication technologies have become available to non-governmental observers and reporters, enhancing their ability to cover ongoing events and to disseminate their views, images, and perspectives on those events.

Indeed, in every major crisis in which the United States has been involved since the end of the Cold War, from Somalia to Bosnia to Haiti to Kosovo, the international media has presented a wide variety of facts, images, and viewpoints additional to, different from, and contradictory to those presented by the U.S. government. This has obvious relevance for military operations and defense policy.

Sometimes, observers and reporters who presented alternative facts and viewpoints reported objectively and were simply doing their jobs. In Somalia, the international media from the beach filmed the unopposed landing of U.S. forces in Mogadishu. This lent a surreal air to the entire operation and raised questions in the American public's eye about the need for the operation. During the Kosovo conflict, reporters in Belgrade quickly covered the U.S. bombing of the Chinese embassy, raising questions about American intent. Other free-lance observers on the ground in Kosovo were among the first to question the U.S. military's original battle damage assessment of casualties inflicted on Serb forces there, raising questions about U.S. honesty. All these reports were accurate, but from the U.S. government's perspective, it would have been better if they had not reached the public at all, much less in real time.

Other times, actors who want to influence U.S. policy to move in a direction in line with their own objectives stage events to be covered by the media. In Bosnia, questions remain to this day about who actually fired mortar shells into a Sarajevo market, killing almost a hundred people. Some maintain that Serbian forces launched the attack; others assert that Bosnian Muslims did it to generate sympathy for their cause.

In Haiti, the military government organized an anti-American mob to appear in port, frustrating an American attempt to land and hoping to raise questions in the U.S. of why an American intervention was contemplated in the first place.

Still other times, those hostile to U.S. policy objectives use the media to their own ends. Again in Somalia, the media broadcast pictures of the body of a U.S. serviceman being dragged through Mogadishu's streets, undermining support in the U.S. for the American presence in Somalia. Similarly, during the Kosovo conflict, Serbia broadcast pictures of collateral damage caused by U.S. attacks to shore up support for the Milosevic regime domestically and increase criticism of the U.S. and NATO internationally.

These alternative viewpoints, facts, and images sometimes raise questions in the United States about the wisdom of an operation or action. Other times, they undermine the ability of U.S. forces in the field to carry out their mission. Almost always, they complicate the situation for U.S. civilian and military policymakers. In the Information Age, this will often be a fact of life for policymakers, who may either ignore this reality, learn to live with it, or seek to turn it to their advantage.

Indeed, given the growing capability of the international media and other actors to provide their interpretations and images of events to broad audiences, Karl von Clausewitz's dictum that "war is the continuation of politics by other means" will become even more relevant in the Information Age than in earlier ages.

Another time-tested dictum is that wars can be won or lost off or on the battlefield. In the Information Age, this will be truer than ever, and it will be equally true for conflicts and crises. “Preparing the battlefield” in the Information Age will be a global exercise that requires that civilian and military decisionmakers pay attention to all aspects of the capabilities that information and communication technologies provide.

Military Operations Will Be Increasingly Integrated

The capabilities provided by ubiquitous information and communication technologies and the demands of the 21st century battlespace will dictate that the U.S. military integrate its operations both horizontally and vertically. This will significantly alter the way in which military operations ranging from main force warfare to operations other than war are conducted.

The U.S. military already recognizes the need for horizontal integration. *Joint Vision 2010* strongly emphasized jointness, or put differently, the horizontal integration of military activities. In addition, the separate service documents presented earlier in this volume often emphasized jointness. Even more importantly, several of the services to one extent or another have also begun to incorporate jointness into their planning, training, and operations.

Nevertheless, given the frequently dominant priorities of service pride and prestige, full horizontal integration of military capabilities remains a thing of the future. A long way must still be traveled before jointness is achieved.

The need for vertical integration is less widely recognized. In some quarters in the U.S. military, it is even opposed. By vertical integration, we mean the linking together of all types of actions that might influence the outcome of a military operation, ranging from the full-scale application of force through command and control warfare on to psychological operations, civil action, and public affairs. Especially in operations other than war, effective vertical integration provides a military operation the best chance for success.

Unfortunately, vertical integration is difficult to achieve and often not fully understood. The military, and sometimes civilian authorities as well, often but not always prefers forceful action, that is, the application of armed force.[5] Many decisionmakers reject psychological operations as unsavory. In addition, civil action and public affairs operations rarely show quick result. Meanwhile, questions remain about the effectiveness and the legality of cyber attacks on opponent's civil infrastructures.[6]

Despite these uncertainties, difficulties, and questions, vertical integration of operations will become a more important part of military operations in the Information Age than it has been in the past, especially for operations other than war. Enhanced ISR, C4I, and PF will all be in the arsenals of Information Age militaries, but so too will closing down enemy communications systems, morphing the images and changing the messages of opponent leaders, electronically degrading or paralyzing an opponent's infrastructure, and communicating directly with an opponent's citizens.

Indeed, if all of the advantages afforded by Information Age technologies are to be fully realized and if full spectrum dominance is to be obtained, horizontal and vertical integration of military operations must be fully ingrained into the thinking, planning, training, and conduct of the U.S. military. This will increasingly be a requirement of successful Information Age defense policy.

Decision Cycles Will Tighten

Information Age technologies will make more accurate information more readily available to U.S. military and political decisionmakers more quickly than ever before. To the extent that this provides an opportunity for U.S. decisionmakers to “get inside” an opponent’s decision loop, the U.S. will acquire a “speed of command” decisionmaking advantage that will allow a command authority to marshal forces and to initiate actions more quickly than an opponent.

The advantages of this are obvious. Seizing the initiative has long been an objective of military commanders. In the Information Age, U.S. commanders more than ever will be able to seize the initiative on the basis of large quantities of highly accurate readily available real time information. But there will be dangers in a tightened decision cycle as well.

First, rapid decisions are not necessarily wise decisions. Sometimes, a wise decision may evolve only after considerable thought, discussion, and analysis. As the ability to make rapid decisions increases, the danger lurks that speed of command will replace wisdom of command as an objective. This is not a new concern, but it is one that will be heightened as Information Age technologies provide more information more rapidly.

Second, the availability of increased quantities of information will increase pressures for automated decisionmaking. In certain situations and under certain conditions, this may be both necessary and wise. But in other situations and under other conditions, automated decisionmaking could be a mistake. The question, then, is “In what situations and under what conditions will it be necessary and wise to automate decisions, and in what situations and under what conditions will it be necessary and wise to retain a human in the decision loop?” This question has no simple answer.

Third, concern will inevitably grow that opponent decisionmakers will also have easy and quick access to large quantities of highly reliable information. This concern will further increase pressure for decisionmakers to make decisions more quickly. The danger, of course, is that this pressure will force premature decisions to be made on the basis of inaccurate, partial information, or inadequate analysis. Even before the Information Age, there were many cases of this. Witness the U.S.S. Vincennes downing of an Iranian Airbus passenger plane because the Vincennes’ battle center believed it to be an Iranian F-14. Obviously, delaying decisions until all is known is an equally flawed approach. We will need to learn to strike the proper balance, waiting when we can and acting when we must.

There is little doubt that Information Age technologies will increase pressures to tighten decision cycles. The first level of importance here, however, is not the speed at which one can make a decision. Rather, it is what one does with the difference in time that exists between the time it takes to complete one’s own decision loop and the time that it takes for an opponent to complete his decision loop. If this time differential is used well, information can be verified, wise decisions more readily reached, and errors minimized. Despite the inevitability of increased pressure for faster decisions in the Information Age, we would do well to remember that accuracy and wisdom, not speed alone, are the objectives of decisionmaking.

The Tempo of Operations Will Increase

During the 1990s, the tempo of operations of the American military increased substantially. Indeed, American military forces were used in support of separate U.S. foreign policy objectives more times during the 1990s than they were in any other decade in American history. There were at least three reasons for this, the first two of which were not directly related to the Information Age.

First, with the collapse of the Soviet Union, the United States reigned supreme as the world's only superpower. No countervailing power existed. Thus, opportunities for using American military power without generating a response from a foreign military power that could truly endanger the United States or its national interests increased significantly. Often, the U.S. acted on those opportunities.

Second, because of the end of the Soviet threat, the U.S. significantly cut the size of its military. This was understandable. Nevertheless, the combination of more opportunities for the use of American armed forces and the reality of fewer deployed forces in the field led to a significant increase in operational tempo.

Third, the increased flow of information from sensors and other intelligence, surveillance, and reconnaissance

(ISR) capabilities combined with improved command, control, communications, computers, and information dissemination (C4I) capabilities and enhanced precision force (PF) applications has led to a faster tactical tempo. More target information will be available in real time, allowing more sorties to be launched. Attacking forces will be re-directed in mid-mission.[7] Precision force capabilities will be delivered from a distance, allowing friendly forces to avoid enemy fire and to initiate more sorties. Focused logistics will permit supplies and weapons to be delivered as needed, reducing downtime as forces wait for supplies. Thus, in every respect, the Information Age will lead to an increased tempo.

This increased tempo of military operations presents a real danger for the U.S. military of the early 21st century. During the 1990s, many observers commented on the stresses that the increased operational tempo placed on American armed forces. Assuming that essentially unopposed interventions remain frequent and that no sizeable expansion in the number of deployable U.S. forces occurs, improved C4ISR and PF capabilities will not only serve as force multipliers, but also increase the stresses on U.S. armed forces that result from more deployments and increased operational and tactical tempo.

Up to a certain undefined point, this does not present a danger. But beyond that undefined point, this is not good for the U.S. military. The necessary art is to find that point and not move beyond it. An increased tempo may increase one's ability to impose one's will on an enemy, but over time, it can also degrade one's own forces.

Network Centric Concepts and Hierarchies Will Coexist

Extensive evidence suggests that the dominant trend in military organization is away from hierarchy toward network centric concepts.[8] However, it is highly unlikely that military hierarchies will disappear. Rather, network centric concepts and hierarchies will coexist in the U.S. and in the armed forces of other states during the Information Age. This will also likely be true in the military organizations and actions of non-state actors.[9]

Network centric concepts are enabled by Information Superiority which is in turn enabled by Information Age technologies. They focus on altering human and organizational behavior by linking organizational assets together in a network to take full advantage of their information and capabilities. In defense policy, network centric concepts seek to derive the maximum amount of combat capabilities from distributed interacting entities by sharing information and on occasion decisionmaking authority. Network centric concepts also help maximize the use of information, increase responsiveness, lower risks, decrease costs, increase the tempo of operations, and increase overall combat effectiveness.

Network centric operations are based on three elements. The first is geographically dispersed forces, the second is knowledgeable forces, and the third is reliable linkages between and among forces. These elements provide enhanced combat potential, reduced levels of risk, and expanded situational flexibility. The linkages that exist between and among one's forces permit the massing of effect that once required the massing of forces. Because network centric forces are geographically dispersed, they offer fewer high value targets. Risk is therefore substantially reduced. At the same time, since all nodes are knowledgeable, operational tasking and responsibility can be dynamically reallocated to adapt to changing situations.

Nevertheless, even though Information Age technologies favor and enable network centric concepts in defense policy, their institutionalization does not mean that traditional hierarchical methods of organization and behavior will fall completely by the wayside. The role of network centric concepts will expand immensely in defense policy in the Information Age but they will coexist with traditional hierarchical concepts.

In part, the survival of hierarchy in the military will be a function of tradition. Throughout history, armed forces have been commanded and controlled by hierarchical systems. Lower ranks have always reported to higher ranks, and each higher rank in turn had a greater level of decisionmaking authority than the rank below it. This tradition will not die easily, especially in the military.

But there is reason beyond tradition that military hierarchies will survive in the network centric Information Age. When disagreements exist about military objectives, strategies, or tactics, hierarchy impose discipline, if not agreement. Whatever else the Information Age brings, it will not bring an end to disagreement over objectives, strategies, or tactics. Hierarchy will thus be required to maintain discipline and resolve disagreements.

Inevitably then, network centric concepts and hierarchies will coexist in Information Age militaries. Tension will exist between them, but ways will be found to make the tension constructive as each serves its separate purposes and each adds its strengths to Information Age armed forces.

The U.S. Military Will Make Mistakes, but It Will Learn from Those Mistakes

If the response of the U.S. military during the first few years of the Information Age is an accurate indication of how it will respond as the Information Age progresses, there is reason for optimism. Led by the Joint Chiefs of Staff and the services, the U.S. military early on began to respond to the potentials and opportunities provided by the technologies of the Information Age and the capabilities that they promised to provide. *Joint Vision 2010* and the accompanying separate service documents goaded the services into accelerating their exploration of the potential that could flow from Information Age technologies. *Joint Vision 2020* continues this process. While some advocates of the revolution in military affairs maintain that the U.S. has not moved rapidly enough to adapt to Information Age concepts, the U.S. military is, in reality, far ahead of the rest of the world.

As we saw in the introduction to this volume, and as the discussions of Somalia, Bosnia, and Kosovo showed, this does not mean that the U.S. military has not made mistakes. Indeed, there is significant room for improvement in many areas. And inevitably, more mistakes will be made as new technologies become available and are incorporated into the inventory.

Mistakes will include errors as elementary as employing new technologies in incorrect ways, as basic as developing inappropriate doctrines and strategies for deployment and use, and as frustrating as overlooking new technologies that may have significant military applications.

As errors and mistakes are rectified and as U.S. military capabilities expand, we may be tempted to believe that Information Age technologies and the capabilities that they provide will eliminate war's fog and friction. Unfortunately, this will not be the case. Rather, fog and friction will only be reduced to levels lower than ever before. And if we learn to take advantage of the opportunities this provides, this is good news. If we forget that fog and light will still exist and do not find ways to accommodate this residual uncertainty and inefficiency, the results could be tragic.

But the best news is that the U.S. military has shown itself willing to incorporate Information Age technologies into its arsenal, develop strategies and doctrines to employ them, and to educate its personnel on their use. Admittedly, not everything is perfect. Some are reluctant to accept change, some are uncomfortable with jointness, and it is not yet clear whether the U.S. armed forces will institute alterations in its organizational structure comprehensive enough to take the fullest advantage of Information Age opportunities. But in many areas, the U.S. military is aware of what is needed to take advantage of Information Age change and is exploring ways to institute change.

Even so, this relatively optimistic assessment does not mean that the United States' armed forces are where they need to be. When it comes to preparing for warfare, conflict, and operations other than war in the Information Age and what they will require, we have begun the journey, but we still have a long way to go.

[1] While the development and deployment of certain types of advanced information-based capabilities as weapons requires extensive technological prowess and large sums of money, the development, deployment, and use of other types of information-based capabilities that could be used as weapons does not.

[2] Here, we must recall Chapter 1's observation that impressive advances are being made directed at energy, stealth, robotics, miniaturization, micro-electro-mechanical systems, biotechnology and bioengineering, molecular biology, non-human behavioral modification, materials, and nanotechnology. Like advances in information and communication technologies, these technologies promise to provide the military forces that obtain them the ability to engage in warfare, conflicts, and operations other than war in truly revolutionary ways. The technologies of the Information Age are not the only ones that will revolutionize military affairs.

[3] As in Volume 2 and in Chapter 1, we differentiate between "challenges" and "threats." "Challenges" refer to attacks on U.S. information and communications systems that fall below the threshold of compromising or degrading the ability of the U.S. military to operate. They do not endanger U.S. national security. "Threats" refer to attacks on information and communications systems that have potential to compromise or degrade the ability of the U.S. military to operate or that do endanger U.S. national security. Admittedly, the dividing line is imprecise. Nevertheless, the distinction is useful in discriminating between different levels of dangers presented by different attacks against and intrusions into U.S. information and communication systems.

[4] See for example James Kitfield, "Command and Control the Messenger," National Journal (September 11, 1999), pp. 2546-2552.

[5] Here one is reminded of General Wesley Clark's observation that if electronic means had been used in conjunction with other non-military measures against Serbia in 1990, military attacks against Serbia might not have been necessary. See Julian Borger, "Cyberwar Could Spare Bombs," *The Guardian*, November 5, 1999, p. 17.

[6] See Bradley Graham, “Cyberwarfare: It’s Still a Pandora’s Box,” *Washington Post*. See also General Counsel, U.S. Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, D.C.: U.S. Department of Defense, 1999).

[7] This occurred during the 1999 Kosovo conflict.

[8] The following discussion of network centric concepts is taken primarily from David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.: U.S. Department of Defense, 1999), pp. 87-122.

[9] For one view of what network centric warfare employed by a non-state actor may look like, see John Arquilla and Theodore Karasik, “Chechnya: A Glimpse of Future Conflict?,” *Studies in Conflict and Terrorism* (Fall 1999), pp. 207-229).

About the Editors

David S. Alberts is currently the Director, Research and Strategic Planning, OASD (C3I). Prior to this he was the Director, Advanced Concepts, Technologies, and Information Strategies (ACTIS), Deputy Director of the Institute for National Strategic Studies, and the executive agent for DoD's Command and Control Research Program. This included responsibility for the Center for Advanced Concepts and Technology (ACT) and the School of Information Warfare and Strategy (SIWS) at the National Defense University. Dr. Alberts has more than 25 years of experience developing and introducing leading edge technology into private and public sector organizations. This extensive applied experience is augmented by a distinguished academic career in computer science and operations research, and Government service in senior policy and management positions.

Daniel S. Papp is Senior Vice Chancellor for Academic Affairs of the University System of Georgia. Before assuming this post, Dr. Papp was Director of Educational Programs for Yamacraw, the State of Georgia's initiative to become the global leader in broadband technologies and components. Dr. Papp has also been Interim President of Southern Polytechnic State University, Executive Assistant to the President at Georgia Tech, and Founding Director of the Georgia Tech School of International Affairs. In addition, Dr. Papp has been Visiting Professor at the Western Australia Institute of Technology; Research Professor at the Strategic Studies Institute of the U.S. Army War College; Senior Research Professor at the Center for Aerospace Doctrine, Research, and Education of the U.S. Air War College; and Visiting Professor at Fudan University in Shanghai. A Phi Beta Kappa graduate of Dartmouth College, Dr. Papp received his Ph.D. from the University of Miami. His academic specialties include international security policy, U.S. and Russian foreign and defense policies, and the impact of information and communciation technologies on national security and the international system. Dr. Papp is the author or editor of nine books and over 60 journal articles and chapters.