INFORMATION DOMINANCE: Special Operations Forces in MOOTW

BY

Lieutenant Colonel Steven A. McCain
United States Air Force

USAWC CLASS OF 1997

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION DOMINANCE: Special Operations Forces in MOOTW

by

Lieutenant Colonel Steven A. McCain
United States Air Force

Colonel Walter R. Berg
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Steven A. McCain, Lt Col, United States Air Force

TITLE: Information Dominance: Special Operations Forces in MOOTW

FORMAT: Strategy Research Project

DATE: 15 April 1997

Three trends are shaping the relationship among Information Operations (IO), special operations forces (SOF), and Military Operations Other Than War (MOOTW). The first trend is the transition of the battlespace toward unconventional warfare with rising global terrorism, drug trafficking, and proliferation of weapons of mass destruction (WMD). The second trend is the mounting pressure to further reduce Department of Defense (DoD) force structure while recapitalizing forces for the future. The third trend is the rapidly improving capability to wage IO worldwide.

This study examines the emerging role of IO relative to missions of the United States Special Operations Command (USSOCOM) in MOOTW. The hypothesis of this paper contends IO, conducted by SOF, should play a more pivotal role in the capability of DoD to support our national objectives as complex MOOTW dominate conflict in the 21st Century. Strategy, policy, operational concepts, and organizational structure must adapt quickly to "information Age" challenges to counter evolving threats to our national security. In a rapidly changing world, SOF must be affordable yet technologically advanced to fully support emerging operational concepts and achieve critical information dominance for America in MOOTW.

TABLE OF CONTENTS

INTRODUCTION

"The one country that can best lead the information revolution will be more powerful than any other."

Joseph S. Nye, Assistant Secretary of Defense for International Affairs; William A. Owens, Vice Chairman, Joint Chiefs of Staff[1]

The purpose of this paper is to examine the emerging role of Information Operations (IO) relative to missions of the United States Special Operations Command (USSOCOM) in Military Operations Other than War (MOOTW). The paper will begin with pertinent definitions, followed by discussion of current issues and trends. Analysis and evaluation of the potential synergy of Special Operations Forces (SOF), IO, and MOOTW will then be discussed in terms of the evolving threat, a smaller Department of Defense, national policy and strategy. Recommendations and conclusions will be offered.

The hypothesis of this paper contends IO, conducted by SOF, should play a more pivotal role in the capability of the Department of Defense to support our national objectives as complex MOOTW dominates conflict in the 21st Century. Strategy, policy, operational concepts, and organizational structure must adapt quickly to "Information Age" challenges to counter evolving threats to our national security. Rising global terrorism, transnational crime, and proliferation of weapons of mass destruction (WMD) threaten our world even as Defense budgets shrink. SOF must be affordable yet technologically advanced to respond to the changing battlespace and achieve critical information dominance for America in future MOOTW.

DEFINITIONS

> *"Coming to grips with information warfare is like the effort of the blind men to discover the nature of the elephant: the one who touched its leg called it a tree, another who touched his tail called it a rope..."*
>
> Martin Libicki, National Defense University[2]

Information Warfare

US National Security Strategy discusses the importance of information to the achievement of our national objectives, of the identification of emerging threats to our information systems, and the need to develop protection strategies.[3] The 1997 US National Military Strategy speaks of winning the information war by leveraging reconnaissance, intelligence, collection and analysis, high-speed data processing and transmission to assure our ability to dominate our adversaries.[4] The Department of Defense defines Information Warfare (IW) as:

> Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our own information... IW is an overarching, integrating strategy... in the command, control and execution of military forces and in the implementation of national policy.[5]

The seven basic forms of IW are defined in Figure 1.

Joint Vision 2010 discusses the vital need for information superiority to meet emerging operational concepts of dominant maneuver, precision engagement, full-dimensional protection, and focused logistics. Information superiority is defined as the ability to ... "collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[6] Both offensive and defensive Information Operations (IO) will be required to achieve such superiority.

IO permeate the full range of military operations integrating all aspects of information to enhance the elements of combat power.[7] Psychological operations (PSYOP), deception, Electronic Warfare (EW), computer network attack, physical destruction, and special information operations (SIO) are used to conduct offensive IO. Defensive IO includes information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, EW, and SIO.[8] IW involves "an IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[9] IW is a means, not an end.

The concepts and terms used in conjunction with IW are still developing. CAPT Gravell, USN, of the Joint Staff Information Assurance Division states ... " the DoD is not yet ready to anchor terminology related to IW and IO".[10] Whatever the final definition, IW has emerged as a key joint warfighting mission area with control of information pivotal to the continuing success of our nation's Armed Forces.[11]

Special Operations

"Special operations (SO) encompass the use of small units in direct or indirect military actions that are focused on strategic and operational objectives."[12] SO are conducted along the entire spectrum of military conflict, including wartime operations and MOOTW, independently or in coordination with conventional forces. JCS pub 1-02 further clarifies SO as:

> Operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or psychological objectives by unconventional military means in hostile, denied, or politically sensitive areas. Political-military considerations frequently shape special operations, requiring clandestine, covert, or low visibility techniques and oversight at the national level.[13]

SOF are designated by the Secretary of Defense to conduct SO and include components from the Army, Air Force, and Navy. The nine principal missions of USSOCOM (see Glossary for definitions) are listed below:

- Counterproliferation (CP)
- Special Reconnaissance (SR)
- Psychological Operations (PSYOP)
- Direct Action (DA)
- Foreign Internal Defense (FID)
- Civil Affairs (CA)
- Combatting Terrorism (CBT)
- Information Operations (IO)
- Unconventional Warfare (UW)[14]

In addition to the principal missions, SOF perform a variety of collateral activities ranging from counterdrug actions to combat search and rescue. SOF provide the National Command Authority (NCA) a highly-trained, rapidly-deployable, joint force capable of conducting a wide range of taskings anywhere in the world.[15]

Military Operations Other Than War

Military Operations Other Than War (MOOTW) includes a wide range of activities conducted to deter war and promote peace.[16] MOOTW can occur before, during, and after war.[17] Joint Pub 3-07 defines MOOTW as ... "the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power ..."[18]

There are 16 types of MOOTW (see Glossary for definitions) ranging from peace operations, to combatting terrorism, to arms control.[19] The full range of military operations, including MOOTW, is shown at Figure 2.[20] A recent study completed by the RAND Corporation found characteristics common to MOOTW include political constraints, restrictive

rules of engagement, and operations in an urban environment. Additionally, MOOTW routinely involve non-governmental organizations, coalition efforts, and the use of SOF.[21]

Current Issues and Trends

"the electron is the ultimate precision guided weapon."

John Deutch, former Director CIA[22]

Three simultaneous trends are shaping the synergistic relationship among IO, SOF, and MOOTW. The first trend is the transition of the battlespace toward unconventional warfare with rising global terrorism, drug trafficking, and proliferation of weapons of mass destruction (WMD). The second trend is the continuing pressure to reduce the DoD force structure while recapitalizing forces for the future. The third trend is the rapidly improving capability to wage IW worldwide.

A Changing Battlespace

The end of the Cold War has fundamentally changed America's security imperatives. Threats today are more diverse and increasingly involve US forces in MOOTW. Along the spectrum of conflict, MOOTW as a means to support our National Security Strategy (NSS) of engagement and enlargement is gaining importance. Non nation-state conflict is on the rise. The threat of terrorism continues to grow. Transnational drug trafficking and crime have reached new heights. The proliferation of WMD and the increasing possibility of their use poses a serious threat to more and more nations. The number of peace operations undertaken to ensure regional stability and control ethnic and religious hatreds is growing.[23]

Future adversaries are likely to be politically, ethically, and legally unrestrained, readily willing to sacrifice innocents to meet their goals.[24] General Sullivan, former Chief of Staff of the Army, describes future operational environments as having greater lethality and dispersion, increased volume and precision of fire. Advanced intelligence technology will provide greater

invisibility for some yet increase detectability of others, with smaller units able to create decisive results.[25]

As we enter an era of strategic IO, with no geographic "front lines," the significance of distance with respect to deployment and use of weapons is reduced.[26] Our borders are no longer impenetrable and everything and everybody is fair game. IW levels the international playing field impacting political, economic, and military power projection. For instance, no single nation can currently challenge US policy using traditional warfare but the US is highly vulnerable to IW attack by an adversary who may or may not claim responsibility. IW attack against a highly information dependent America has already begun.[27] The cost to the US of IW attack has been estimated to be as high as $100-300 billion per year and growing.[28]

IW will redefine the battlespace in ways yet to be discovered. Future SO and IO will blur the traditional distinctions between strategic, operational, and tactical operations.[29] IW departs from the concept of attrition of enemy forces and destruction of physical targets on a linear battlefield. IW emphasizes effects both in and outside the battlespace, of lethal and non-lethal measures, in a non-linear fashion.[30] Economics is replacing territory in global competition and the vector to economic power and military victory is information.[31]

Restructuring the DoD

New priorities and the realities of "downsizing" are changing the size of the Armed forces and the organizational structure of the military institutions. DoD reductions are seen as a politically expedient way to balance the federal budget and reduce the nation's deficit in the near-term. Currently, the Armed Forces are smaller than at any time in the last 45 years.[32] Despite a 70 percent reduction in acquisition and a 45 percent budget reduction from 1985 levels,[33] the US

public has rising expectations of success and an intolerance for casualties, which drive the need for surgical strike capability and short conflict duration. To meet the expectations of the American people, US forces continue to modernize and increase integration of service capabilities.[34]

Eliot A. Cohen, Professor of Strategic Studies at Johns Hopkins University recently stated ... "The new military will be an increasingly joint force--or perhaps, one might say, less and less a traditional, service-oriented force."[35] In countries around the world the traditional separation of the military into armies, navies, and air forces has begun to break down. Air and naval operations have become inseparable from almost any action on the ground. "Quasi" service organizations oriented toward SOF, space operations, and IW are growing in all militarily sophisticated countries.[36]

Although the technology of warfare has altered the relative importance of land, air, and sea power, technology alone will not lead to revolutionary increases in force capability. Changes must occur in doctrine, training, leader development, and organization to fully leverage information technologies to our advantage.[37] A comprehensive review of the military is currently underway, offering a significant opportunity to analyze the role of SOF and IW in future conflict. The Pentagon's Quadrennial Defense Review (QDR) is examining defense strategy, force structure, modernization plans, infrastructure, and readiness. The National Defense Panel will scrutinize the findings of the QDR. Hopefully, Cold War thinking will not dominate the review process, as the emergence of an asymmetrical threat to marginalize US conventional strength appears to be most likely in the near future.[38]

The important questions of who will take the lead for IO within DoD and how DoD will interface with outside agencies during IO is currently being debated. The future effectiveness of IO will be heavily dependent on the ability of the National Security Agency (NSA), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), the DoD and others to successfully share resources in the interagency process.[39] The Defense Science Board Task Force on Information Warfare-Defense (IW-D) recently recommended the SECDEF designate the Assistant Secretary of Defense for C3I as the focal point for coordination of IW. The new focal point would be charged with integration of policy, doctrine, and practice and serve as the key interface for IW interagency activities. The task force also suggests the eventual need for a Under Secretary of Defense for Information and calls for immediate funding and implementation of 50 actions to improve functioning of IW within the DoD.[40] How much to centralize and under whom, to effectively develop an IW strategy, is still a highly contentious issue within DoD.

The US Government and the DoD are aggressively pursuing defensive and offensive IW initiatives. For example, Executive Order 13010--Critical Infrastructure Protection, established a commission to oversee development of a national strategy to protect our national interests.[41] US Attorney General Janet Reno recently asked her fellow Cabinet members, including the Secretaries of Commerce, Energy, Treasury, Transportation, the CIA and FBI directors, and the Assistant Secretary of Defense, to create a national cyberspace defense "entity" and establish a cyberwar defense policy board.[42]

DoD is spending $3 billion over the next four years to safeguard its information systems.[43] The Chairman Joint Chiefs of Staff is expanding IW functioning in J3 and the Joint Information Warfare Center (JIWC). The JIWC will be staffed around the clock and interface

with the CINCs IW cells, the Joint Spectrum Center, the Joint Warfare Analysis Center, the Joint Command and Control Warfare Center, and the Service IW organizations.[44]

Advancing Information Technology

Improved detection, prioritization, and assessment of information and precision of combat power employment are all a result of advancing information technology. Most, if not all, of our emerging weapons technologies rely increasingly on the integration of information technologies. A global network linking computers and information functions to each other by fiber-optic and satellite links, will eventually allow almost instantaneous communication to anyone else, anywhere in the world.[45] The microprocessor has brought us into the "Information Age." The rate of increase of computing power is currently 4,000 times per decade for a given unit of cost.[46] Logic would dictate this particular rate cannot continue indefinitely. "All components of the global information network are growing exponentially."[47] The rapid integration of information technology is impacting all areas of governments and societies as information becomes the capital commodity of the future.[48]

New commercial-of-the-shelf (COTS) technologies are affordable and thus available to anti-western organizations. Information technologies are linking our transnational adversaries with significant IW capabilities.[49] The ability to insert airborne computer viruses into enemy computers is being studied and could have significant implications regarding both offensive and defensive IW.[50] New "cruise viruses" are like a smart info weapon. Their purpose is to capture specific data or destroy a specific hard disk. Once introduced into a network of computers, the virus waits until "triggered" to attack its specified target. Additionally, new software programs can not only replicate themselves once inserted into a computer network but can also alter their

own structure automatically over time. Defense against the new "evolutionary" computer viruses will be difficult.[51] Super Quantum Interference Devices (SQUIDs) which read human brain waves may one day lead to the direct insertion of information into the brain of an adversary from afar.[52] The possibilities are astounding and too numerous to mention here.

Proliferation of information technologies is outstripping information security with dire consequences for the US. As technology advances so does our dependence on information systems and our vulnerability to information warfare attack. In most US facilities, command and communications nodes are not well hidden and are vulnerable to precision strike.[53] Although C2 vulnerability has been reduced by the rapidly falling cost of bandwidth and redundancy. Conversely, expansion of cellular nodes makes effective C2 communications denial difficult. Multiple channels of electronic access complicates both psychological operations and electronic countermeasures.[54]

The US will retain a significant edge in space and systems integration for the near-term.[55] Recent advances in the integration of command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) systems gives decision makers a more accurate understanding of the battlespace more quickly than ever before. For the first time, C4ISR architecture is being developed before the weapon systems designed to operate within this new architecture.[56]

New enabling technologies are becoming available for warfighters now. A world wide, three dimensional, digital map will provide a common reference system vital to sensors and fusion of data for C2, planning, and operational execution. Advanced multispectral and hyperspectral sensors will facilitate automatic change recognition (ACR) technologies which can

provide vital warning systems. Enhanced battlespace awareness technologies link unmanned autonomous vehicle (UAV) sensors to the joint surveillance target attack radar system (JSTARS), providing real-time video of operations activity.[57] The Defense Advanced Research Projects Agency (DARPA) is crafting a strategic response to ensure the DoD can achieve information superiority into the 21st century. DARPA is developing smaller, lighter, and more mobile information systems. They are focusing on electronics where 40 percent of the life-cycle cost of many weapon systems occurs. Technology base development programs are increasingly geared to dual civil-military use. DARPA believes that military research efforts should look beyond the immediate horizon and capitalize on the short-term absence of a near-peer competitor.[58]

Analysis and Evaluation

"... the struggle for power changes when knowledge about knowledge becomes the prime source of power."

... Alvin Toffler[59]

Focusing the analysis of information operations, special operations, and MOOTW in three key areas reveals both challenges and benefits in the near future. First, the complementary characteristics of IO and SO as force multipliers and as providers of response options to counter an evolving threat are evaluated. Secondly, the impact of changing missions and DoD "downsizing" upon organizational structures is reviewed. Finally, the metamorphosis of national policy and strategy that must occur to successfully implement emerging military capabilities is discussed.

Mission Response to an Evolving Threat

Serious security challenges of the near future are most likely to involve MOOTW. SOF must develop both offensive and defensive IW capabilities to meet the evolving threat. SO should embrace IW to ensure continued relevance as conventional forces develop capabilities previously associated only with SOF. The natural synergy between IO and SO should lead to innovative force application in future MOOTW and to attainment of US national objectives.[60]

The primary focus of IO in support of a MOOTW should be to preserve the peace, deter escalation of conflict, and prepare the battlefield for offensive IW should the crisis escalate.[61] IO strategy and implementation "may have its greatest impact in peace and the initial stages of crisis."[62] IO supports US strategic policies by improving the effectiveness of deterrence and influencing the perceptions and decision making of others. Our use of information-based warfare (IBW) provides an additional option more likely to be acceptable in political and diplomatic

channels and more congruent with our national will. Superior knowledge of the battlespace also enables policymakers to act sooner to contain or deter a crisis. Proactive use of information superiority provides a wider range of indirect and nonlethal measures to achieve political outcomes. IBW can provide a potent tool to promote stability and thwart aggression via the use of knowledge as power.[63]

Information-based warfare also complements our nuclear deterrent. Controlling access to critical information gives the US and her allies significant advantage in achieving national objectives, including the non-proliferation of WMD.[64] SOF's contribution to counter-proliferation of WMD can be enhanced by integrating their principal missions of IO, direct action, special reconnaissance, and PSYOPS. "SOF can be effective early in the weapon acquisition cycle to monitor, deter, or delay the cycle as well as later to deter, prevent, or protect against weapon use."[65]

Computers may well be the weapon of choice for terrorists in the near future. Accessing a computer network offers a cheap, quick, and reliable method to attack vital NII. Such attacks can be plausibly denied and are especially effective against the industrialized "west." "The odds of getting caught are low, of being prosecuted lower still."[66] Future IW attacks by international terrorist organizations could be effectively countered by SOF trained to combat IW outside US sovereign territory.[67]

To avoid direct confrontation with US strengths, adversaries may attempt indirect attack by focusing on weaker US allies in order to create US domestic upheaval and expense. Examples might include the disruption of Mexico's less-protected computer financial network to undermine their economy or assisting with the communications requirements of Latin American

drug cartels.[68] Alternatively, US drug interdiction could be supported by disrupting drug cartel lines of communications and financial networks or by conducting a PSYOP campaign with the goal of isolating the adversary from external support.[69]

The regional orientation of SOF is responsive to US Commanders-in-Chief while the strategic flexibility of SOF is responsive to the National Command Authority.

> A global political setting characterized by political fragmentation, in which enemies and friends may be difficult to identify, is likely to be ideally suited for the use of SOF... We will need special operations forces to operate behind an enemy's front lines, to attack targets of major importance, to integrate reconnaissance and intelligence efforts, to establish clandestine and unconventional operations...[70]

SOF can be surgically targeted and rapidly deployed to any location worldwide providing theater CINCs with IO options to prepare the battlespace. The ability of SOF to penetrate hostile or denied territory is critical for offensive IW operations where ready access to an adversary's networks is not possible.

Many of the characteristics common to SOF are needed for successful implementation of IO. SOF have a shortened chain of command to speed response to crises while maintaining operations security. SOF also have considerable experience wedding interagency operations so critical to effective IO execution. Both IO and SO require discrete, low-profile, intelligence-oriented actions to effectively support MOOTW. Additionally, SOF personnel are linguistically trained and culturally attuned, and politically sensitive which enhances their value for MOOTW. IO and SO can involve indirect tactical actions of strategic significance. SOF are inherently joint, often combined, and capable of forming small, versatile, self-contained teams to meet information dominance requirements.[71]

Advanced information technologies make it possible for small teams of combatants to have the capability of a C3I communications node.[72] To eliminate such a powerful and mobile adversary will require the mobility and potential lethality that SOF provides. Urban warfare and streetfighter confrontation is on the rise and will not be bloodless as many analysts predict. Terrorists attack may focus on the will of the US and play on our aversion to casualties.[73] Hostage-taking and indiscriminate attack will require a specialized force capable of fighting terrorists on their own turf. SOF must continue to embrace unorthodox approaches, including the application of emerging IO capabilities, is vital to combating unconventional adversaries.[74]

Organizational Change

What the current QDR and future NDP reviews should suggest is less duplication of military capabilities in a declining budget environment. Elimination of parallel capability must be matched by increased synergy among the services and related government agencies. The potential impact of IO and SO on DoD structure is not expected to be seriously considered until the next QDR;[75] however, organizational and conceptual changes will gain momentum in the next few years as the potential impact of emerging operations is better understood.

The information revolution and the emergence of IW as both a capability and a threat to critical national infrastructures will change the DoD and the interagency process of which it is part. IO as an integrating strategy requires a seamless interface among agencies, services, departments, and programs. The Defense Information Infrastructure (DII) of communications networks, computers, software, databases, applications, data, and other information processing capabilities stretches across the entire spectrum of conflict. It is widely recognized that existing "stovepipe" information systems and organizations will have difficulty meeting future needs of

the warfighter. A reduction in IO classification regarding the "who" and the "what" will be required in order to cut across "stovepipes" and achieve mission success. Establishment of a multi-agency IO technology center could improve integration of new technologies, standardize systems, and realize cost savings. Additionally, some argue the need for the National Security Council (NSC) to establish an organization to parcel out IO responsibilities to agencies and a strengthened Joint Staff organization to orchestrate IO within DoD to improve IO processes.[76]

An important way Congress controls agency interaction, and thus organizational structure, is through the budget and the Economy Act, which requires each agency to reimburse other agencies for any services provided. Currently, this act inhibits the effective cooperation of agencies during IO where clear roles are difficult to establish and dollars are tight. The decision as to who takes the lead role and who provides support in a counter-terrorism (CT) IO, for example, is not always obvious. For traditional CT, the NSC takes overall responsibility then assigns the Department of State for overseas operations or FBI for US only activity; however, IW does not lend itself well to clear-cut agency assignment. Often no single agency has total responsibility, authority, capability to meet IO taskings.[77]

Government and private sectors must work to together to resolve many of the issues related to defense of our NII and infiltration of adversary information infrastructure.[78] Eventually the US may create an organization headed by an "IW Czar" but for the near term, at least, the NSC will appoint a lead agency to coordinate with the growing number of players needed to work a national IO effectively.[79] Certainly benefit can be gained by merging offensive and defensive IO activities under single organizations within the various government agencies as

in the Joint Staff where the J3 provides the CINCs an office of primary responsibility for IO matters.[80]

Within USSOCOM, sub-commands have developed varying levels of competence regarding IO execution. Theater Special Operations Commands (SOCs), however, are not yet fully integrated with IW theater campaign plans. Joint Task Force (JTF) organizational structure now calls for an IO cell as part of the JTF staff to assist with IO integration with the larger JTF mission. The Joint Force Air Component Commander (JFACC) and the SOC Air Control Element linkage to the IO cell needs improvement. The use of SOF and IW liaisons in the JFACC to work issues for the Joint Targeting Coordination Board should prove beneficial to future operations.[81] New organizations are creating demand for IO specialists. USSOCOM is examining an Army study which proposes three primary career paths, one of which includes development of IO personnel.[82]

"Future defense budgets will demand cost-effective solutions. Because of its low cost/high payback ratio, SOF will continue to be called upon."[83] SOF manning is relatively small when compared to conventional force requirements enhancing their desirability. The information revolution can also be leveraged for high payback and lends itself to a smaller, flatter DoD. Many would argue information connectivity improves the ability to mass forces quickly at the precise location they are needed and thereby reduces overall conventional force requirements. Obviously there are limits to how far this logic can be applied as physical mass on the ground is still an imperative for many situations.[84]

The military's large, traditional, function-oriented, pyramidal structures should be reevaluated. Business has shown that smaller process-oriented horizontal structures work well in

an information intensive environment.[85] Currently, an Army corps organizational chart looks more like the organization of General Motors in the 1950s than a cutting-edge corporation of today like Motorola.[86] Tremendous flexibility is needed to rapidly direct actions in complex military operations. Careful review of hierarchy, span of control, response time, and centralization is needed. I3W will change the way we approach conflict, much like the tank and the airplane have done previously. New approaches will require radical restructuring to fully implement an effective National military IW strategy.[87]

National Strategy and Policy

Any strategy for IW and its integration with SOF must be fully supportive of the broader NSS and the NMS (see Figure 3). The NSS directs that strong intelligence capabilities and defense be maintained, to include specialized units.[88] The NMS directs the Armed Forces to "win the information war."[89] Additionally, strategy should fit within the conceptual template provided by Joint Vision 2010 to leverage information based technologies and IW in the next century.[90] JV2010 stops short of specifying how responsibility for information dominance is to be parceled out among the services but, clearly establishes the central importance of information superiority to emerging operational concepts.[91]

Information operations must become accepted as integral to combat and as more than combat support. Achieving information dominance will require greater fusion of Operations and Intelligence functions within an advanced C4ISR framework. It is essential that all the services fully exploit and integrate IW concepts.[92] Effective strategies to counter growing IO threats are being implemented. General Shelton, CINC USSOCOM, states:

> Our emphasis in the rapidly evolving IO mission includes continued development of targeting methodology (links, nodes, human factors), determining intelligence requirements, assessing hostile/friendly

vulnerabilities, and identifying coordination requirements to operationalize IO strategies.[93]

Any future strategy must also be based on national policy. Attempts to develop a National Information Policy and answer difficult questions about the changing nature of IW are being addressed by a growing number of government and private organizations. The President's National Security Telecommunications Advisory Committee (NSTAC) provides a private industry perspective to the executive branch on National Security. NSTAC has assigned a task force to review NII and information assurance.[94]

Policy must determine who will maintain control of our NII and develop procedures for integration with our DII.[95] Currently, 95 percent of DoD communications ride on public switched networks wherein DoD has little ability to control or influence security standards.[96] Current limitations on the DoD to provide a viable defensive capability for our NII leaves us open to attack by the many forces who wish to topple the US.[97] NMS dictates that US forces project power beyond our national boundaries. Such projection requires policy development for long-distance, globally fused information systems.[98]

Policy must clarify whether an information attack against our industry or economic interests is an attack against the US itself.[99] Additionally, who pulls the IW "trigger" must be determined.[100] Current national policy requires National Security Council (NSC) approval for IW actions which support non-military elements of power or fall into the category of national strategy. Theater operational control of IW has been delegated to the CINC. Rules of engagement (ROE) for IW activity are especially difficult in a MOOTW scenario, as is the question of how much information to share with our coalition partners. International and US

laws are often non-specific or overly restrictive, making IO implementation difficult. For instance, the US Privacy Act severely limits our actions against adversaries, even in the US.[161]

Information is non-linear, can be used by both sides at the same time, and is hard to measure and retain advantage over, making protection extremely difficult.[162] A new capstone policy should emphasize security and a basic framework for networking, interoperability, and distribution strategies.[163] Policy should integrate the media with other aspects of IO to US benefit, as technology provides journalists access to every detail of a MOOTW. The "press" will increasingly serve as the "poor man's" intelligence service.[164]

Acquiring information technologies will require a systematic acquisition strategy. The relative value of military research and development (R&D) projects as compared to private industry efforts, commercial of the shelf (COTS) systems, or direct intelligence sources, must be established. Unlike in the past, today's technical breakthroughs come faster in the civilian sector than in defense-related R&D. This change calls for a strategic reexamination of priorities and a restructuring between military and civilian science and technology.[165] The gap between leading-edge technologies and in-use technologies must be bridged quickly to ensure successful application of IW by SOF in the "Information Age". DII prototyping, Joint Warrior Interoperability Demonstrations, and COTS evaluations provide the means for rapid migration of technologies to mission application. DISA and ARPA have joined to form an Advanced Information Technology Services Joint Program Office which will further expedite transition of technology to warfighting capability.[166]

Until recently, no truly overarching national strategy for the implementation of IW existed. A significant step toward such a strategy occurred with the completion of DoD

Directive 3600.1. The opportunity now exists for USSOCOM to develop a "line of authority" regarding IW. The Joint Staff, as the lead agent for DoD in developing joint doctrine, completed Joint Pub 3-13 (First Draft) on "Information Operations" in February 1997.[107] The draft publication lists responsibilities (see appendix 3) for USSOCOM based on DoD Directive 3600.1 and Chairman, Joint Chiefs of Staff Instruction 3210.01, "Joint IW Policy."[108]

USSOCOM should determine the capabilities required to meet these potential new responsibilities now. A mission need statement on Joint IW, validated by the Joint Requirements Oversight Council (JROC) in October 1996, provides a vehicle for the services and USSOCOM to develop requirements.[109] Using major force program 11 (MFP-11) USCINCSOC can allocate the necessary resources to create new capabilities in outyear budgets based on the defined line of authority. The separate MFP provides freedom to react quickly and greater visibility of SOF's multi-service programs to the DoD and to the Congress.[110]

Recommendations and Conclusions

"We must have Information Superiority...Information Superiority will require both offensive and defensive information warfare."

Joint Vision 2010[11]

Recommendations

The transition of the DoD and USSOCOM to meet a radically different future must be accelerated. Improved interagency coordination between government, industry, and private organizations are a must if the full potential of SOF coupled with IW is to be fully realized. Recommended actions include:

- Establish multi-agency IO Technology Center to include USSOCOM liaison
- Increase resources for IO within the DoD Joint Staff and USSOCOM
- Full review of SO and IO impact on DoD structure during QDR and NDP
- Develop national policy and doctrine which better integrates NII and DII and establishes interagency procedures to enhance SOF execution of IO mission
- Reduce levels of access whenever possible to improve interagency functions
- Establish laws that increase the government's freedom to respond to IO attack
- Strengthen acquisition "line of authority" linking SOF, IO, national policy
  - USSOCOM determine responsibilities, required capabilities, and required resources to implement tasings listed in JCS pub 3-13
  - USSOCOM establish training program to meet new IO responsibilities
  - Focus SOF recapitalization on C4ISR systems integration
- Create a deployable IW Unit in USSOCOM to serve as a catalyst for rapid implementation of unorthodox IW strategies, tactics, and procedures, increase SOF awareness of IW capabilities and vulnerabilities
- Establish IO career path where personnel receive experience in multi-disciplinary areas (i.e. PSYOPS, public affairs, intelligence, JTF IO cell staff)

In the near term, the DoD should continue to concentrate its efforts in defensive IW but not to the exclusion of offensive IW. SOF should aggressively integrate IO concepts to counter an asymmetrical attack aimed at US informational vulnerabilities and to bolster their strategic relevance in a changing world.

Conclusions

Currently, the United States has a window of opportunity to prepare for the future. With no near-peer competitor, a healthy economy, and military and technological preeminence, the time to exploit new information technologies and develop new military strategies is now. We can no longer afford to spend as much of our scarce resources on "industrial age" weaponry but should concentrate our efforts to leverage "information age" capabilities and concepts.

Converging trends indicate a rising need for SO, IO, and MOOTW in the near future. A favorable synergy among these types of operations and continuing budgetary pressures will provide the "critical mass" for DoD reorganization and function within the next 15 years. DoD will be smaller, flatter, more horizontal, less centralized, and more dependent on SO and IO. By increasing emphasis on IO, USSOCOM will integrate critical leading-edge IW capabilities providing low-profile, versatile, and politically-sensitive options for our national leadership. US strategic dominance will increasingly depend on our informational advantage and our ability to employ SOF along the entire spectrum of conflict, especially in MOOTW, well into the next millennium.

GLOSSARY

Terms for Special Operations Forces Principal Missions[112]

Civil Affairs (CA): Activities that establish, maintain, influence, or exploit relations between military forces and civil authorities to facilitate military operations.

Combatting Terrorism (CBT): Offensive and defensive measures to preclude, preempt, and resolve terrorist actions throughout the entire threat spectrum.

Counterproliferation (CP): Actions taken to seize, destroy, capture, or recover weapons of mass destruction, including the application of military power to protect US forces and interests; intelligence collection and analysis; and support of diplomacy, arms control, and export controls. Accomplishment of stated activities may require coordination with other US government agencies.

Direct Action (DA): Short-duration strikes, and other small-scale offensive actions to seize, destroy, capture, recover, or inflict damage on designated personnel or material.

Foreign Internal Defense (FID): Assist, organize, train, and advise host nation military and paramilitary forces to enable them to free and protect their societies from subversion, lawlessness, and insurgency.

Information Operations (IO): Actions taken to achieve information superiority I support of national military strategy by affecting adversary information systems while leveraging and protecting US information and information systems.

Psychological Operations (PSYOP): Activities to convey selected information to foreign audiences t induce or reinforce foreign attitudes and behaviors favorable t originator's objectives.

Special Reconnaissance (SR): Actions to obtain or verify, by visual observation or other collection methods, information concerning the capabilities, intentions, and activities of an actual or potential enemy; or to secure data concerning the characteristics of a particular area.

Unconventional Warfare (UW): Support to military and paramilitary operations, normally of long duration, predominately conducted by indigenous or surrogate forces. Includes guerrilla warfare and other offensive, low-visibility operations.

Terms for Military Operations Other Than War[113]

Arms Control: A concept that connotes: (a) any plan, arrangement, or process, resting upon explicit or implicit international agreement, governing any aspect of the following: the numbers, types, and performance characteristics of weapon systems (including the command and control, logistics support arrangements, and any related intelligence-gathering mechanism); and the numerical strength, organization, equipment, deployment, or employment of the Armed Forces retained by the parties (it encompasses disarmament); and, (b) on some occasions, those measures taken for the purpose of reducing instability in the military environment.

Combatting Terrorism: Actions, including anti-terrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum.

DOD support to counterdrug operations: Support provided by the Department of Defense to law enforcement agencies to detect, monitor, and counter the production, trafficking, and use of illegal drugs.

Enforcing an Exclusion Zone: A zone established by a sanctioning body to prohibit specific activities in a specific geographic area. The purpose may be to persuade nations or groups to modify their behavior to meet the desires of the sanctioning body or face continued imposition of sanctions, or use or threat of force.

Ensuring Freedom of Navigation: Operations conducted to demonstrate US or international rights to navigate air or sea routes.

Humanitarian Assistance: Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by US forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing humanitarian assistance.

Military support to civil authorities: Those activities and measures taken by the DOD Components to foster mutual assistance and support between the Department of Defense and any civil government agency in planning or preparedness for, or in the application of resources for response to, the consequences of civil emergencies or attacks, including national security emergencies. Also called MSCA.

Nation Assistance: Civil and/or military assistance rendered to a nation by foreign forces within that nation's territory during peacetime, crises or emergencies, or war based on agreements mutually concluded between nations. Nation assistance programs include, but are not limited to, security assistance, foreign internal defense, other US Code Title 10 (DOD) programs, and activities performed on a reimbursable basis by Federal agencies or international organizations.

Noncombatant Evacuation Operations: Operations conducted to relocate threatened noncombatants from locations in a foreign country. These operations normally involve US citizens whose lives are in danger, and may also include selected foreign nationals. Also called NEO.

Peace Operations: Encompasses peacekeeping operations and peace enforcement operations conducted in support of diplomatic efforts to establish and maintain peace.

Protection of shipping: The use of proportionate force by US warships, military aircraft, and other forces, when necessary for the protection of US flag vessels and aircraft, US citizens (whether embarked in US or foreign vessels), and their property against unlawful violence. This protection may be extended to foreign flag vessels, aircraft, and persons consistent with international law.

Recovery Operations: Operations conducted to search for, locate, identify, rescue, and return personnel or human remains, sensitive equipment, or items critical to national security.

Show of force: An operation, designed to demonstrate US resolve, which involves increased visibility of US deployed forces in an attempt to defuse a specific situation, that if allowed to continue, may be detrimental to US interests or national objectives.

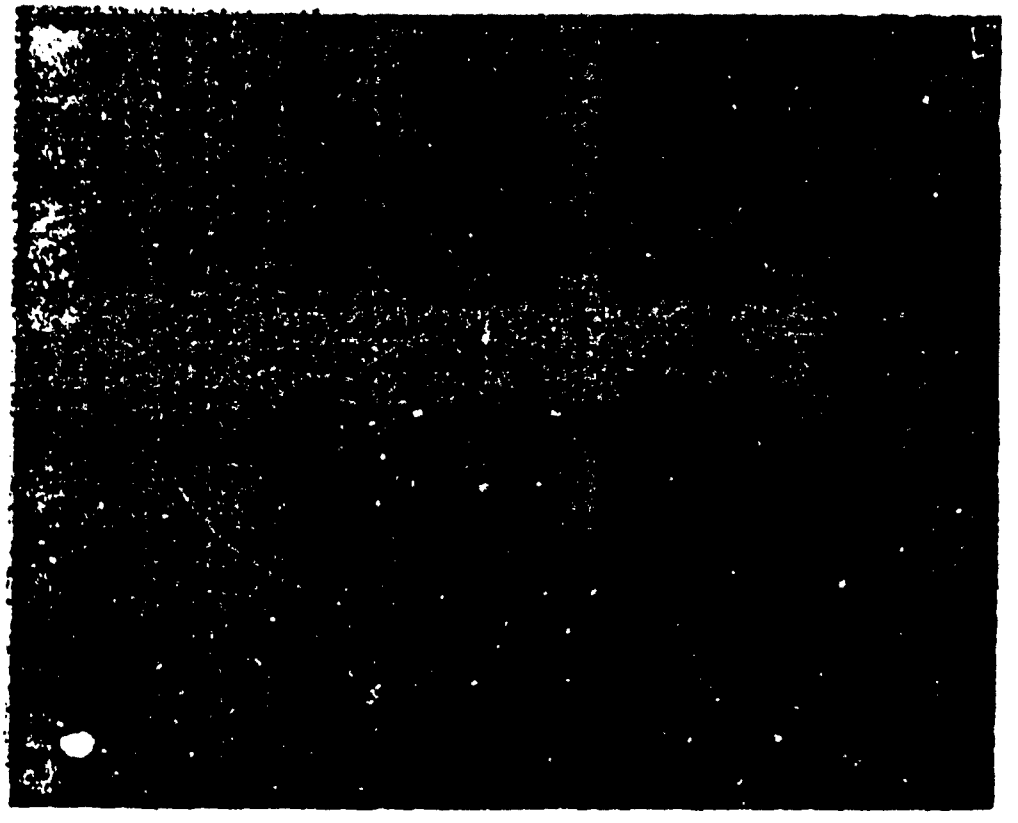
Strike and Raids. Raid: An operation, usually small scale, involving a swift penetration of hostile territory to secure information, confuse the enemy, or to destroy installations. It ends with a planned withdrawal upon completion of the assigned mission. **Strike:** An attack which is intended to inflict damage on, seize, or destroy an objective.

Support to insurgency: Support provided to an organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict. Support to counterinsurgency: Support provided to a government in the military, paramilitary, political, economic, psychological, and civic actions it undertakes to defeat insurgency.

ILLUSTRATIONS

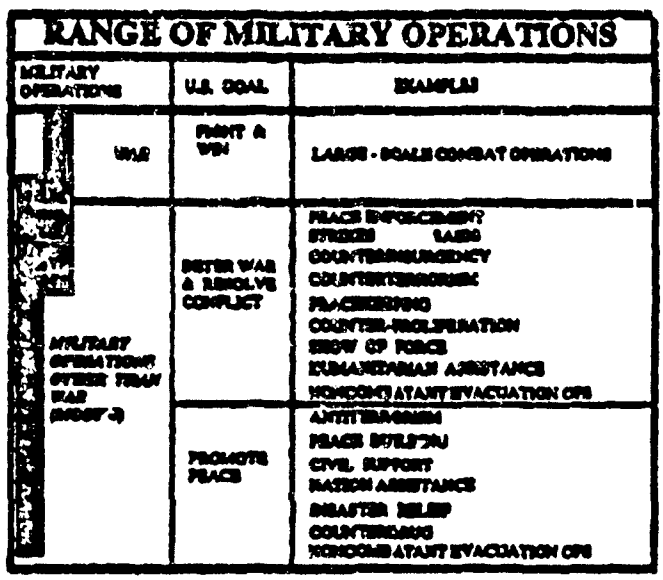
Figure 1

INFORMATION WARFARE



Source: National Defense University, Institute for National Strategic Studies, "Strategic Assessment 1996: Instruments of National Power," Washington GPO, p. 194.

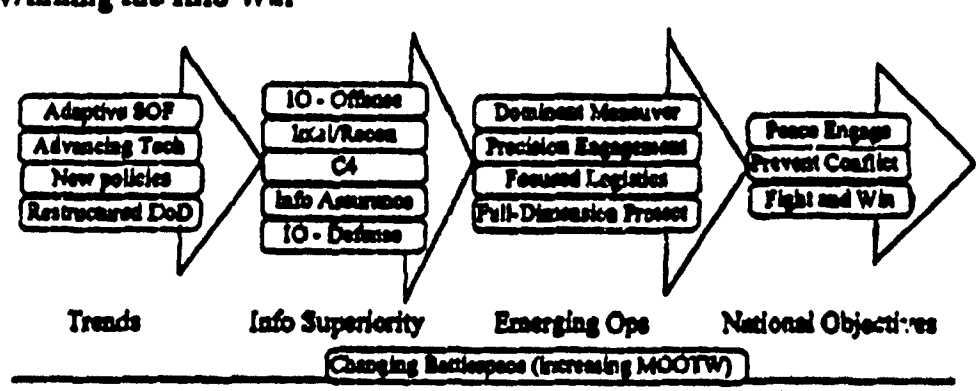
Figure 2



Source: John F. Kennedy School of Government, "Roads to New Strength: Preparing Leaders for Military Operations Other Than War," *National Security Program Policy Analysis Paper 94-02*, Harvard University, 1994, p.2.

Figure 3

Winning the Info War



Source: Adapted from US Joint Chiefs of Staff, Joint Vision 2010, and Information Warfare-Special Tactical Operations Division briefing, 13 February 1997.

Figure 4

Joint Doctrine for Information Operations
Responsibilities of Commander in Chief, USSOCOM

1. Conduct research, development, testing and evaluation, and procurement of IO capabilities that meet validated Service and Joint requirements.

2. Maintain liaison with Services, Defense agencies, and other appropriate agencies to minimize duplication of IO capabilities.

3. Identify intelligence requirements applicable to IO capabilities being developed or fielded. Coordinate with Defense Intelligence Agency (DIA) and the Joint Staff to ensure these requirements are communicated to the Intelligence Community.

4. Incorporate IO into Service school curricula and into appropriate training and education activities. Both offensive and defensive aspects of IO must be addressed.

5. Organize forces with IO capabilities. Train forces to conduct IO (to include IW). Ensure Services' IO forces and capabilities effectively support the combatant commanders through the appropriate Service component commanders.

6. Exercise IO capabilities across the range of military operations.

7. Coordinate with DIA, Defense Information Systems Agency (DISA), and NSA to ensure development and population of databases supporting collaborative planning, analysis, and execution of IO.

8. As required, develop Service IO policy, doctrine, and tactics that complement emerging joint doctrine.

Source: United States Joint Chiefs of Staff, Joint Pub 3-13 (First Draft), Pentagon, Washington DC, 21 January 1997, pp. I-10 thru I-11.

ENDNOTES

[1]Joseph S. Nye Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs*, March/April, 1996, Vol. 75, No. 2, p. 20.

[2]Martin C. Libicki, "What is Information Warfare?," Draft Version, Advanced Command Concepts and Technology, Institute for Strategic Studies, National Defense University, 21 July 1995, p. 2.

[3]The White House, Office of the President of the United States, *A National Security Strategy of Engagement and Enlargement*, Washington GPO, February 1996, pp. 24-25.

[4]United States Joint Chiefs of Staff, *National Military Strategy of the United States of America*, Washington GPO, 1996, p. 15.

[5]Richard Power, "CSI Special Report on Information Warfare", *Computer Security Journal*, Vol. 11, no. 2, San Francisco, CA, p. 2.

[6]United States Joint Chiefs of Staff, "Joint Vision 2010: America's Military Preparing for Tomorrow", *Joint Force Quarterly*, Summer 1996, no. 12, p. 41.

[7]Department of the Army, Field Manual 100-6, *Information Operations*, August 1996.

[8]Department of Defense Directive (DODD) S-3600.1, *Information Operations*, December 1996.

[9]United States Joint Chiefs of Staff, Joint Pub. 3-13 (First Draft), *Joint Doctrine for Information Operations*, Washington Government Printing Office (GPO), 21 January 1997, p. I-18.

[10]William Gravell, Captain, USN, United States Joint Chiefs of Staff, Information Assurance Division, *Defensive Information Warfare*, briefing to US Army War College, 30 January, 1997.

[11]United States Joint Chiefs of Staff, White Paper, *Information Warfare: A Strategy for Peace... The Decisive Edge in War*, 1996, p. executive introduction by General John M. Shalikashvili, Chairman Joint Chiefs of Staff.

[12]United States Special Operations Command, Pub. 1, *Special Operations in Peace and War*, 25 January 1996, p. 1-2.

[13]United States Joint Chiefs of Staff, Pub. 1-02, *DoD Dictionary of Military and Associated Terms*, Washington GPO, 23 March 1994, pp. 404-405.

[14]Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, "United States Special Operations Forces," *1996 Posture Statement*, pp. 31-32.

[15]Henry H. Shelton, General, USA, Commander in Chief, United States Special Operations Command, briefing to US Army War College, Carlisle Barracks, 12 February, 1997.

[16]Ronald J. Bath, Lt Col, ANG, *et al.*, "Roads to New Strength: Preparing Leaders for Military Operations Other Than War," John F. Kennedy School of Government, *National Security Program Policy Analysis Paper 94-02*, Harvard University, 1994, p. 3.

[17]United States Joint Chiefs of Staff, Joint Pub. 1-02, "DoD Dictionary of Military and Associated Terms, Washington GPO, 23 March 1994, p. 265.

[18]United States Joint Chiefs of Staff, Joint Pub. 3-07, *Joint Doctrine for Military Operations Other Than War*, Washington GPO, 7 January 1995, p. GL-3.

[19]Ibid., p. III-1.

[20]Bath, p. 2.

[21]Jennifer Morrison Taw and John E. Peters, *Operations Other Than War: Implications for the U.S. Army*, Arroyo Center, prepared for the U.S. Army by Rand, 1994, p. 8.

[22]John Deutch, Director, Central Intelligence Agency, Internet, Information Warfare Links Page, <http: // members.aol.com/tomlnn8054/information/html>, 25 June, 1996.

[23]Daniel P. Bolger, Lt Col, USA, *Savage Peace: Americans at War in the 1990s*, Novato CA, Presidio Press, 1995, pp. 50-56.

[24]Charles J. Dunlap Jr., Colonel, USAF, "Sometimes the Dragon Wins: A Perspective on Information-Age Warfare," *Infowar.Com & Interpact*, Inc., 1996, pp. 1-4.

[25]Gordon R. Sullivan and Anthony M. Coroalles, "The Army in the Information Age," *Carlisle Barracks: Strategic Studies Institute*, 31 March 1995, pp. 3-4.

[26]Roger C. Molander, *et al.*, "Strategic Information Warfare: A New Face of War," *Parameters*, US Army War College Quarterly, Vol. XXVI, No. 3, Autumn 1996, pp. 85, 92.

[27]Stuart E. Johnson, *et al.*, "Dominant Battlespace Knowledge: The Winning Edge," *Institute for National Strategic Studies*, National Defense University Press, Washington DC, October 1995, p. 11.

[28]Winn Schwartau, "Information Warfare: Chaos on the Electronic Superhighway," Thunder's Mouth Press, New York, 1994, p. 16.

[29]National Training Center, Louisiana Maneuvers, "Information Operations 2010", *Force XXI briefing*, 1996, p. 15.

[30]Lawrence E. Casper, et al., "Knowledge-Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly*, Autumn 1996, No. 13, p. 84.

[31]Gravell.

[32]United States Joint Chiefs of Staff, "Joint Vision 2010: America's Military Preparing for Tomorrow," *Joint Force Quarterly*, Summer 1996, No. 12, p. 38.

[33]Norman Augustine, Chief Executive Officer and Vice Chairman, Lockheed Corporation, briefing to US Army War College, Carlisle Barracks, PA, 7 November, 1995.

[34]Eliot A. Cohen, "A Revolution in Warfare", *Foreign Affairs*, Vol. 75, No. 2, pp. 47-48.

[35]Ibid., p. 47.

[36]Ibid., pp. 47-48.

[37]Douglas Macgregor, "Breaking the Phalanx: A New Design for Landpower in the 21st Century," Westport Connecticut, Praeger, 1997, Chapter III.

[38]Dennis Ippolito, Chairman, Department of Political Science, Southern Methodist University, briefing to US Army War College, Carlisle Barracks, PA, 13 November, 1996.

[39]United States Joint Chiefs of Staff, "Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance," Washington GPO, 2nd edition, 2 July 1995.

[40]Defense Science Board Task Force, "Information Warfare - Defense," Office of the Under Secretary of Defense for Acquisition and Technology, Washington DC, November 1996, p. 6-2.

[41]Presidential Documents, "Executive Order 13010--Critical Infrastructure Protection," *Executive Order 13010 of July 15*, 1996, Federal Register: July 17, 1996, Vol. 61, No. 138, pp. 37345-37350.

[42]Robert F. Minehart, National Security Agency, Visiting Professor US Army War College, interview by author 12 February 1997, Carlisle Barracks, PA.

[43]Jack Weible, "Vulnerable to Attack: Subcommittees get an earful on threats to information systems," *Air Force Times*, April 14, 1997, p. 28.

[44]Defense Science Board Task Force, p. 6-6.

[45]John L. Peterson, "The Road to 2015: Profiles of the Future," Waite Group Press, CA, 1994, p. 33.

[46]Ibid., p. 30.

[47]Ibid., p. 34.

[48]Ibid., p. 39.

[49]Dunlap, p. 4,5.

[50]Schwartau, p. 253.

[51]Alvin and Heidi Toffler, "War and Anti-War," Warner Books Inc., New York, May 1995, p. 177.

[52]Schwartau, p. 360.

[53]Ibid., p. 252.

[54]Martin Libicki, CDR James Hazlett, et al., "The Revolution in Military Affairs: Conference Conclusions," *National Defense University*, Strategic Forum, Institute for National Strategic Studies, pp. 1-4.

[55]Ibid., p. 3.

[56]Casper, p. 84.

[57]Ibid., p. 87.

[58]Lance A. Glasser, Director Electronics Technology Office, Defense Advanced Research Projects Agency, "Today's Technology Begets Tomorrow's Military Readiness," internet, DARPA ETO Home Page, 1996, pp. 1-3.

[59]Alvin Toffler, I-War Research Group Information Warfare Media Labs, internet, <http://www.i-war.com>, 1996.

[60]United States Special Operations Command, "SOF Vision 2020," pp.2-5.

[61]United States Joint Chiefs of Staff, Information Assurance Division, *Defensive Information Warfare*, briefing slides, 1997, p. 13.

[62]Ibid., p. 5.

[63]Casper, p. 85.

[64]Ibid.

[65]Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, "United States Special Operations Forces," *1996 Posture Statement*, p. 27.

[66]Schwartau, p. 22.

[67]Johnnie H. Wauchop, Colonel, USAF, interview by author 28 January 1997. (Note: Col Wauchop currently assigned to the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, Washington DC.

[68]Charles J. Dunlap Jr., Colonel, USAF, "Sometimes the Dragon Wins: A Perspective on Information-Age Warfare," *Infowar.Com & Interpact*, Inc., 1996, p. 2.

[69]Gravell.

[70]Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, "United States Special Operations Forces," *1996 Posture Statement*, p. 28.

[71]United States Special Operations Command, Pub. 1, Special Operations in Peace and War, 25 January, 1996, pp. 2-29, 2-30.

[72]Dunlap, p. 3.

[73]Ibid., pp. 2-4.

[74]National Defense University, Institute for National Strategic Studies, "Strategic Assessment 1996: Instruments of National Power," Washington GPO, pp. 148-151.

[75]Henry H. Shelton, General, Commander in Chief, US Special Operations Command, interview by author, 20 February 1997, Carlisle Barracks PA, and Charles Tamburello, Captain, USN, US Joint Chiefs of Staff, J38, Special Technical Operations Division, interview by author, 13 February 1997, Carlisle Barracks PA.

[76]Chuck Tamburello, Captain, USN, United States Joint Chiefs of Staff, Information Warfare-Special Tactical Operations Division briefing, 13 February 1997.

[77]Wauchop.

[78]Presidential Documents, "Executive Order 13010--Critical Infrastructure Protection," *Executive Order 13010 of July 15*, 1996, Federal Register: July 17, 1996, Vol. 61, No. 138, p. 37346.

[79]Wauchop.

[80]Internet, Information Warfare tutorial, "Executive Summary," <http:// CARLISLE-WWW.ARMY.MIL/usacsl/iw/tutorial/execsum.htm>, 24 October 1996, p. 1.

[81]Sam Dick, Lieutenant Colonel, USAF, USSOCOM, Information Warfare Branch, interview by author, 3 January 1997.

[82]Henry H. Shelton, General, Commander in Chief, US Special Operations Command, interview by author, 20 February 1997, Carlisle Barracks PA.

[83]Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, p. 28.

[84]Center for Strategic and International Studies, Leading Edge Warfare Working Group, Report on Session 3, 22 January, 1997.

[85]Libicki, Hazlett, p. 3.

[86]E. Cohen, pp 47-48.

[87]Toffler, p. 179.

[88]The White House, Office of the President of the United States, *A National Security Strategy of Engagement and Enlargement*, Washington GPO, February 1996, pp. 13, 23.

[89]United States Joint Chiefs of Staff, *National Military Strategy of the United States of America*, Washington GPO, 1996, p. 15.

[90]John M. Shalikashvili, General, USA, Chairman Joint Chiefs of Staff, "A Word From the Chairman," *Joint Force Quarterly*, Summer 1996, No. 12, pp. 1-5.

[91]United States Joint Chiefs of Staff, "Joint Vision 2010: America's Military Preparing for Tomorrow", *Joint Force Quarterly*, Summer 1996, no. 12, pp.34-49.

[95]Sandra I. Meadows, "Information Dominance Anchors Vision of Joint Warfare in 2010," *National Defense*, December 1996, Vol. LXXXII, No. 523, pp.12-13.

[96]Henry H. Shelton, General, Commander in Chief, US Special Operations Command, interview by author, 20 February 1997, Carlisle Barracks PA.

[97]The President's National Security Telecommunications Advisory Committee, "Fact Sheet," 23 February 1996.

[98]Schwartau, p. 25.

[99]Internet, Information Warfare tutorial, "DoD Roles and Missions," <http://CARLISLE-WWW.ARMY.MIL/usacsl/iw/tutorial/mod3.htm>, 24 October 1996, p. 1.

[100]Gravell.

[101]Leonard Tabacchi, Defense Information Systems Agency, Defense Information Infrastructure Master Plan Manager, , "Executive Summary," *Defense Information Infrastructure Master Plan*, 6 November 1995, pp. 1-6.

[102]Schwartau, p. 25.

[103]Internet, Information Warfare tutorial, "IW Weapons," <http://CARLISLE-WWW.ARMY.MIL /usacsl / iw/tutorial/mod6.htm>, 24 October 1996, p. 3.

[104]Waschop.

[105]Toffler, p. 167.

[106]Schwartau.

[107]Dunlap, p. 9.

[108]Toffler, p. 167.

[109]Tabacchi, p. 5.

[110]United States Joint Chiefs of Staff, Joint Pub. 3-13 (First Draft), 21 January, 1997.

[111]Ibid., pp. 10, 11.

[112]Tamburello.

[113]Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, p. 29.

[111]Chairman Joint Chiefs of Staff, "Joint Vision 2010," Pentagon, Washington DC, 1996, p. 16.

[112]Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, pp. 31-32.

[113]United States Joint Chiefs of Staff, Joint Pub. 3-07, pp. GL-3 thru GL-5.

BIBLIOGRAPHY

Augustine, Norman, Chief Executive Officer and Vice Chairman, Lockheed Corporation, briefing to US Army War College, Carlisle Barracks, PA, 7 November, 1996.

Bath, Ronald J., Lieutenant Colonel, ANG, *et al.*, "Roads to New Strength: Preparing Leaders for Military Operations Other Than War," John F. Kennedy School of Government, *National Security Program Policy Analysis Paper 94-02*, Harvard University, 1994.

Bolger, Daniel P., Lieutenant Colonel, USA, *Savage Peace: Americans at War in the 1990s*, Novato CA, Presidio Press, 1995.

Casper, Lawrence E., et al., "Knowledge-Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly*, Autumn 1996, No. 13, p. 84.

Chairman of the Joint Chiefs of Staff, "Joint Vision 2010," Pentagon, Washington DC, 1996.

Cohen, Eliot A., "A Revolution in Warfare", *Foreign Affairs*, Vol. 75, No. 2.

Center for Strategic and International Studies, Leading Edge Warfare Working Group, Report on Session 3, 22 January, 1997.

Department of Defense Directive (DODD) S-3600.1, *Information Operations*, December 1996.

Department of the Army, Field Manual 100-6, *Information Operations*, August 1996.

Deutch, John, Director, Central Intelligence Agency, Internet, Information Warfare Links Page, <http: // members.aol.com/teambun8054/information/html>, 25 June 1996.

Defense Science Board Task Force, "Information Warfare - Defense," Office of the Under Secretary of Defense for Acquisition and Technology, Washington DC, November 1996.

Dick, Samuel, Lieutenant Colonel, USAF, USSOCOM, Chief, Information Warfare Branch, interview by author, 3 January 1997.

Dunlap, Charles J., Jr., Colonel, USAF, "Sometimes the Dragon Wins: A Perspective on Information-Age Warfare," *Infowar.Com & Interpact*, Inc., 1996.

Glasser, Lance A., Director Electronics Technology Office, Defense Advanced Research Projects Agency, "Today's Technology Begets Tomorrow's Military Readiness," Internet, DARPA ETO Home Page, 1996.

Gravell, William, Captain, USN, United States Joint Chiefs of Staff, Information Assurance Division, *Defensive Information Warfare*, briefing to US Army War College, Carlisle Barracks, PA, 30 January, 1997.

Internet, Information Warfare tutorial, "Executive Summary," <http:// CARLISLE-WWW.ARMY.MIL/usacsl/iw/tutorial/execsum.htm>, 24 October 1996.
Internet, Information Warfare tutorial, "DoD Roles and Missions," <http:// CARLISLE-WWW.ARMY.MIL/usacsl/iw/tutorial/mod3.htm>, 24 October 1996.

Internet, Information Warfare tutorial, "IW Weapons," <http://CARLISLE-WWW.ARMY.MIL /usacsl / iw/tutorial/mod6.htm>, 24 October 1996.

Ippolito, Dennis, Chairman, Department of Political Science, Southern Methodist University, briefing to US Army War College, Carlisle Barracks, PA, 13 November, 1996.

Johnson, Stuart E., *et al.*, "Dominant Battlespace Knowledge: The Winning Edge," *Institute for National Strategic Studies*, National Defense University Press, Washington DC, October 1995.

Libicki, Martin C., "What is Information Warfare?," Draft Version, Advanced Command Concepts and Technology, Institute for Strategic Studies, National Defense University, 21 July 1995.

Libicki, Martin, Hazlett, James, CDR, et al., "The Revolution in Military Affairs: Conference Conclusions," *National Defense University*, Strategic Forum, Institute for National Strategic Studies.

Macgregor, Douglas, "Breaking the Phalanx: A New Design for Landpower in the 21st Century," Westport Connecticut, Praeger, 1997.

Meadows, Sandra I., "Information Dominance Anchors Vision of Joint Warfare in 2010," *National Defense*, December 1996, Vol. LXXXII, No. 523.

Minehart, Robert F., National Security Agency, Visiting Professor U.S. Army War College, interview by author 12 February 1997, Carlisle Barracks, PA

Molander, Roger C., *et al.*, "Strategic Information Warfare: A New Face of War," *Parameters*, US Army War College Quarterly, Vol. XXVI, No. 3, Autumn 1996.

National Training Center, Louisiana Maneuvers, "Information Operations 2010", *Force XXI briefing*, 1996.

National Defense University, Institute for National Strategic Studies, "Strategic Assessment 1996: Instruments of National Power," Washington GPO.

Nye, Joseph S., Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs*, March/April, 1996, Vol. 75, No. 2.

Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, "United States Special Operations Forces," *1996 Posture Statement*.

Petersen, John L., "The Road to 2015: Profiles of the Future," Waite Group Press, CA, 1994.

Power, Richard, "CSI Special Report on Information Warfare", *Computer Security Journal*, Vol. 11, no. 2, San Francisco, CA.

Presidential Documents, "Executive Order 13010--Critical Infrastructure Protection," *Executive Order 13010 of July 15*, 1996, Federal Register: July 17, 1996, Vol. 61, No. 138.

Schwartau, Winn, "Information Warfare: Chaos on the Electronic Superhighway," Thunder's Mouth Press, New York, 1994.

Shelton, Henry H., General, USA, Commander-in-Chief, United States Special Operations Command, briefing to US Army War College, Carlisle Barracks, 12 February 1997.

Shelton, Henry H., General, Commander in Chief, US Special Operations Command, interview by author, 20 February 1997, Carlisle Barracks PA, and Charles Tamburello, Captain, USN, US Joint Chiefs of Staff, J38 Special Technical Operations Division, interview by author, 13 February 1997, Carlisle Barracks PA.

Shalikashvili, John M., General, USA, Chairman Joint Chiefs of Staff, "A Word From the Chairman," *Joint Force Quarterly*, Summer 1996, No. 12.

Sullivan, Gordon R. and Anthony M. Coroalles, "The Army in the Information Age," *Carlisle Barracks: Strategic Studies Institute*, 31 March 1995.

Tamburello, Chuck, Captain, USN, United States Joint Chiefs of Staff, Chief, Information Warfare-Special Technical Operations Division, briefing, US Army War College, Carlisle Barracks, 13 February 1997.

Taw, Jennifer Morrison and John E. Peters, *Operations Other Than War: Implications for the U.S. Army*, Arroyo Center, prepared for the U.S. Army by Rand, 1994.

The President's National Security Telecommunications Advisory Committee, "Fact Sheet," 23 February 1996.

The White House, Office of the President of the United States, *A National Security Strategy of Engagement and Enlargement*, Wshington GPO, February 1996.

Toffler, Alvin, I-War Research Group Information Warfare Media Labs, Internet, <http://www.i-war.com>, 1996.

Toffler, Alvin and Heidi, "War and Anti-War," Warner Books Inc., New York, May 1995.

Tabacchi, Leonard, Defense Information Systems Agency, Defense Information Infrastructure Master Plan Manager, "Executive Summary," *Defense Information Infrastructure Master Plan*, 6 November 1995.

United States Joint Chiefs of Staff, Information Assurance Division, *Defensive Information Warfare*, briefing slides, 1997.

United States Joint Chiefs of Staff, Joint Pub. 1-02, *DoD Dictionary of Military and Associated Terms*, Washington GPO, 23 March 1994.

United States Joint Chiefs of Staff, Joint Pub. 3-13 (First Draft), *Joint Doctrine for Information Operations*, Washington Government Printing Office (GPO), 21 January 1997.

United States Joint Chiefs of Staff, Joint Pub. 3-07, *Joint Doctrine for Military Operations Other Than War*, Washington GPO, 7 January 1995.

United States Joint Chiefs of Staff, "Joint Vision 2010: America's Military Preparing for Tomorrow", *Joint Force Quarterly*, Summer 1996, no. 12.

United States Joint Chiefs of Staff, White Paper, *Information Warfare: A Strategy for Peace... The Decisive Edge in War*, 1996, p. executive introduction by General John M. Shalikashvili, Chairman Joint Chiefs of Staff.

United States Joint Chiefs of Staff, "Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance," Washington GPO, 2nd edition, 2 July 1996

United States Joint Chiefs of Staff, *National Military Strategy of the United States of America*, Washington GPO, 1996.

United States Special Operations Command, Pub. 1, *Special Operations in Peace and War*, 25 January 1996.

Wauchop, Johnnie E., Colonel, USAF, Director, Special Activities, Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, Pentagon, Washington DC, interview by author 28 January 1997.

Weible, Jack, "Vulnerable to Attack: Subcommittees get an earful on threats to information systems," *Air Force Times*, April 14, 1997.

REPRODUCTION QUALITY NOTICE

We use state-of-the-art high speed document scanning and reproduction equipment. In addition, we employ stringent quality control techniques at each stage of the scanning and reproduction process to ensure that our document reproduction is as true to the original as current scanning and reproduction technology allows. However, the following original document conditions may adversely affect Computer Output Microfiche (COM) and/or print reproduction:

- Pages smaller or larger than 8.5 inches x 11 inches.
- Pages with background color or light colored printing.
- Pages with smaller than 8 point type or poor printing.
- Pages with continuous tone material or color photographs.
- Very old material printed on poor quality or deteriorating paper.

If you are dissatisfied with the reproduction quality of any document that we provide, particularly those not exhibiting any of the above conditions, please feel free to contact our Directorate of User Services at (703) 767-9066/9068 or DSN 427-9066/9068 for refund or replacement.

END SCANNED DOCUMENT