AU/ACSC/97-0603G/28-377

INFORMATION DOMINANCE

CAN WE AFFORD IT?

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Major Johnny W. Bray

March 1997

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense.

Contents

Preface

In May 1996, CJCS approved a Joint Vision 2010 to serve as the benchmark for Service and unified command visions. The vision's centerpiece is the importance of information superiority as an enabler of new operational concepts. Information superiority is not a new concept, but the methods for obtaining superiority are significantly different. Information superiority is critical now and will be more important in the future. Forward thinking political and military writers and shapers of tomorrow's battlefield have deemed information superiority is an essential element to a successful campaign. This paper provides a pragmatic view of the impact the quest for information superiority may have on the military as a whole and on its individual services. What impact is the quest for information dominance having on our capability to fight and win before we reach 2010?

I would like to thank Lieutenant Colonels James Near and Timothy Ryan, USAF, sponsors of the ACSC Information Warfare Elective, for all their help and insight. I also wish to thank Lieutenant Colonel Steven Torrence, USAF, for serving as my faculty research advisor.

Abstract

Information superiority is one of the United States Air Force's (USAF) six core competencies. Although delineated as a USAF core competency, it is no less important to other Services. In fact, each Service strives to obtain information that will ensure its battlefield success. Their goal is to dominate all campaign areas such as air and fire superiority. This paper focuses on information warfare (IW) and its subset, information dominance (ID), and whether or not the United States or its military can afford it. This paper seeks to answer the following questions: What does the US give up to obtain and maintain ID? What will it cost? Does the US have the forces to meet the operational tempo as we trade personnel power for technology? Does the US need information dominance, especially offensively, against second and third world countries, or should it put resources into active defense? Does the US need defensive and offensive modes of information dominance; can we afford both? Are we headed for information "overkill" to gain information supremacy of the battlefield?

With all the attention given to information gathering following DESERT STORM, and subsequent mis-information regarding IW effectiveness (precision guided missiles, steel on target), the US and its military are caught up in a futurist whirlwind. Futurists, planners, strategists, and thinkers agree the next major threat is 10-20 years away and the US must prepare itself for the 21st century and its dynamic battlefields. If true, don't the US and its military services have the opportunity to take their time and approach

information superiority with forethought? Many experts do not want to give up proven weaponry and capabilities to support what may prove to be only a fad. This paper examines many pragmatists' views on information warfare and information dominance.

Chapter 1

Information Warfare—Hype Or Salvation?

In order to win, we should operate at a faster tempo or rhythm than our adversaries to get inside the adversary's OODA Loop.

—Colonel John Boyd, USAF
Organic Design for Command and Control

Fad addiction is an American characteristic and the US is continuing the trend in government and business.[1] "Information warfare has become so expansive a term that it now threatens to become a tautology by encompassing nearly everything beyond the most primitive forms of combat."[2] The 'line in the sand' once drawn by our leaders has become muddled with the political attractiveness of non-lethal forms of warfare. "The most dangerous legacy of the Persian Gulf War [is] the fantasy of near-bloodless use of force."[3] Colonel Alan Campen writes, "knowledge dominance, as a war-winning strategy, has overwhelming visceral appeal. It induces visions of an inexpensive, a decisive, and a relatively bloodless way to prevent or minimize armed conflicts or to terminate them quickly." He further states this quest is impeded by a lack of historical precedent, common definitions, doctrine, or principles.[4] It may rank right up there with political correctness, for it may be nothing more than a beltway buzzword for electronic warfare.[5] Pierre M. Sprey, military consultant, says that "the Persian Gulf War was won by high

technology has become a cliché, endlessly repeated by journalists ignorant of war and technology advocates living off defense dollars."[6]

War is still about violence, and the illusion new weapons can eliminate the horrors of war is irrational.[7] Information technology cannot be a panacea. Yes, it will allow 20 airplanes to have the capability of 40, but 20 cannot be in 40 "hot spots" at the same time. The military is hurrying to restructure under IW when it has no real coherent IW strategy. Many experts believe information operations and IW will shape the military of the future, or certainly fill some gaping holes left from downsizing its forces. Therefore, Pentagon planners have begun to reflect on this complex, changing reality: dealing with a reduced threat, declining budgets, international conflicts, and still shaping the forces and budgets of the US military in the 21st century.[8]

Information War

> *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 friction and the fog of war can never be eliminated, new technology promises to mitigate their impact.*
>
> —Joint Vision 2010

There is no official IW doctrine and the descriptions of command and control warfare (C^2W) remain incomplete. This paper primarily deals with the strategic and operational levels of IW and ID, but invariably crosses into the tactical arena. Though the lines of delineation are often unclear, that has little relevancy. The intent is to step back from the

publicity and reconsider the military's haste to build an "information warfare bridge" to the 21st century.

There are two streams of thought on the nature and uses of IW. One stresses digitization of the battlefield, a doctrine being tested in the *Force XXI* exercises being conducted in Fort Hood, Texas. The second is that IW is becoming an alternative to more traditional forms of war.[9] It permeates all levels of conflict, from sophisticated tactical electronic warfare to strategic attacks against civil and military information infrastructure.[10]

Basic arguments seem to involve the extent of IW's scope. Although primary emphasis concerns the ability to obtain ID, it is set in the context of IW, or information operations (FM 100-6). Does ID entail defending from an "electronic Pearl Harbor" against our computers and related information systems, or the ability to enable our forces while denying our adversaries? ID is frequently cited as a goal of information warfare.[11] Information technologies should allow us to create a mismatch between our forces and the opponent. "Is there a way we could use information, like current theories of airpower, to create an 'information campaign' that engages an opponent simultaneously in time, space, and depth across the full range of his strategic structures so that the result is strategic paralysis?"[12]

There are more vocal advocates for moving 'full-speed ahead' with information technology than those speaking out for due caution, and that may be understandable with expanding commitments and reduced resources. On the strategic or national front, the IW revolution could put at risk high value national assets outside the traditional battlefield which could affect both national military strategy and broader US national security

strategy.[13] This reason alone gives credence to taking IW seriously and is not a point of contention. The solution may lie in identifying and developing force multipliers to allow US forces to achieve more while making do with less. ID will allow a lean American military to serve and protect its country's still-extensive interests in a world fraught with peril.[14] Information technology will change the way we do battle in the future. However, a precipitous rush to embrace a relatively new, poorly understood, controversial, and unproved strategy is risky. "Information warfare perches precariously on assumptions that, if faulty, would turn a salutary revolution in military affairs into a gamble with national security."[15] Hence, there are numerous reasons why the process must be carefully implemented over an appropriate period of time.

Information Dominance

> *Information dominance is something that is battled for, like air superiority. It is a way of increasing our capabilities by using that information to make correct decisions, and applying them faster than our enemy can. It is a way to alter the enemy's entire perception of reality. It is a method of using all information at our disposal to predict and affect what happens tomorrow, before the bad guy even jumps out of bed and thinks about what to do that day.*
>
> —Major General Kenneth A. Minihan, USAF
> Commander, Air Intelligence Agency

As outlined in Joint Vision 2010, full dimensional protection will be built upon information superiority. Information superiority or dominance may be the thread that holds the conceptual template for how America's armed forces will fight the Joint fight.[16] The USAF has adopted information superiority as one of its six core competencies. Although so delineated, it is no less important to each of the other Services. In fact, armed forces have always striven to obtain the key elements of information that will

ensure success on the battlefield. Each Service will inherently try to dominate the battlefield by gaining superiority on the ground and in the air and space. But what do we have to give up in the short term to obtain ID now and in the future?

The US Armed Forces are the best in the world and there is no room for second place. Even before the Gulf War began, the DOD found itself in the middle of a drawdown. It was expected and inevitable, but the pace has left even the most hardened critic leery of our military posture and ability to support two simultaneous major regional conflicts. The Quadrennial Defense Review report (to be released this Spring) will likely reveal even deeper cuts. The drawdown of personnel and organizational structure may save the taxpayer billions of dollars, but leaves the Services defending not only their force structure but their reason for being.

Throughout history, while knowing more has certainly help influence the battle outcome, ID alone has rarely generated sufficient conditions for winning. For example, the Persian forces failed against Xenophon's hoplite because they couldn't cope with the Greek phalanx, and the Vietcong and NVA, though in a position to initiate actions under favorable conditions, never prevailed against American firepower.[17] In an issue paper written by the RAND Corporation for the USAF, Glenn Buchan says, "pursuing information dominance as a specific operational objective provides both military commanders and analysts with incentives to focus on the wrong part of the problem and confuse overall means and ends..." There is a danger we may lose sight that these type operations must compete with other missions for priority and resources.[18]

Therefore, this paper focuses on ID and whether or not the US can afford it. What do the US and its military have to give up to have ID? What will it cost? The cost cannot

only be addressed in terms of the budget (where it is just short of astronomical), but we must question the potential for another Task Force Smith, or "hollow force" while we trade personnel for technology. Does the US need information dominance, especially offensively, against second and third world countries, or should it put resources into active defense? Does the US need defensive and offensive modes of information dominance; can we afford both? Are we headed for information "overkill" to gain information supremacy of the battlefield?

Following DESERT STORM, and subsequent mis-information regarding information warfare effectiveness (precision guided missiles, steel on target), the US and its military are caught up in a futurist whirlwind. Where is the threat? Futurists, planners, strategists, and thinkers agree the next major threat is 10-20 years away and the US must prepare itself for the 21st century and its dynamic battlefields. If true, the US and military services have the opportunity to take time and approach information superiority with forethought.

There is no question the US has entered a new era and it is imperative the political, social, and military structures embrace the so called "information age." If historical timelines are an indication (each succeeding age [agricultural age, industrial age] has had a shorter time period) the information age may be over before we get the doctrine written.[19] The dilemma the DOD faces in light of the Bottom Up Review (BUR) and suspected outcomes of the QDR, is how to sustain capability in the short term while preparing for the future.[20] The FY97 budget continues the ten-year trend in reduced procurement, a 70 percent decline in dollars, and an overall budget reduction of 45 percent.[21]

The world is in a new age, catapulted by technology at a dizzying pace. If there is no recognizable major threat in the next couple of decades, the US should slow down and

catch its breath. The US must address its own vulnerabilities, dependence on technology, insatiable appetite for information, and capacity to absorb, discern, disseminate and act upon information. What (or who) is driving the train? Technology shouldn't be its own governing force.

The question of ID will be open-ended for some time to come. But can we truly control cyberspace, or is it a conception of our ignorance or arrogance?[22] This paper cannot begin to address all of the questions, nor the hundreds not mentioned. The bottom line—up front—the US can obtain ID strategically, operationally, and tactically, but at what cost?

Notes

[1] R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal* 9, no. 4 (Winter 1995): 69.

[2] Ibid., 73

[3] Steven Aftergood, "The Soft-Kill Fallacy," *The Bulletin of Atomic Scientist* 50, (September-October 1994): 42

[4] Colonel Alan D. Campen, "Rush to Information-Based Warfare Gambles with National Security," *Signal* 49, no. 11 (July 1995): 67

[5] Colonel Alan D. Campen, "Assessments Necessary in Coming to Terms with Information War," *Signal* 50, no. 10 (June 1996): 47

[6] George F. Watson, ed., "The Challenge of Post-Gulf Conflicts," *IEEE Spectrum*, September 1991, 53

[7] Glenn Buchan, *Information War and the Air Force: Wave of the Future? Current Fad?*, RAND Issue Paper 149 (Santa Monica, Calif.: RAND, March 1996), 10 n.p.; on-line, Internet, 14 February 1997, available from http://www.RAND.org// publications/IP/IP149/ index.html.

[8] Watson, 55

[9] DiNardo, 72

[10] Thomas G. Mahnken, "War in the Information Age," *Joint Force Quarterly: JFQ* 10 (Winter 1995-96): 40

[11] Buchan, 3.

[12] George J. Stein, "Information Warfare," *Airpower Journal* 9, no. 1 (Spring 1995): 37.

[13] Roger C. Molander and others. "Strategic Information Warfare: A New Face of War," *Parameters* 26, no. 3 (Autumn 1996): 83. (Original source is RAND Report Mr-661-OSD, 1996).

Notes

[14] John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review*, Summer 1994, 24.

[15] Campen, 67

[16] Joint Chiefs of Staff, *Joint Vision 2010,* 15.

[17] Arquilla, 25.

[18] Buchan, 3-4.

[19] John L. Petersen, *The Road to 2015* (Corte Madera, Calif.: Waite Group Press, 1994), 4-7.

[20] Lawrence E. Casper and others. "Knowledge-Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly: JFQ* 13 (Autumn 96): 81

[21] James Kitfield, "Fit to Fight?" *National Journal*, vol. 28, no. 11 (March 16, 1996): 582.

[22] Colonel Alan D. Campen, "Assessments Necessary in Coming to Terms with Information War," *Signal* 50, no. 10 (June 1996): 47.

Chapter 2

Where Should Our Emphasis Be—Offense, Defense, or Both?

> *We anticipate that cyberwar, like war in Clausewitz's view, may be a "chameleon." It will be adaptable to varying contexts; it will not represent or impose a single, structured approach. Cyberwar may be fought offensively and defensively, at the strategic or tactical levels. It will span the gamut of intensity, from conflicts waged by heavy mechanized forces across wide theaters, to counterinsurgencies where "the mobility of the boot" may be the prime means of maneuver.*
>
> —J. Arquilla and D. Ronfeldt
> *Cyberwar is Coming!*

The President charged the intelligence community, in the National Military Strategy of Engagement and Enlargement, to provide worldwide capabilities to gather timely intelligence on current and emerging information technologies or infrastructure that may potentially threaten US interests at home or abroad.[1] While this sounds like a defensive posture, IW is multi-dimensional, containing offensive and defensive components. More important, it crosses all levels of conflict, runs from the strategic to the tactical and back, and has private and public dimensions.[2] IW, or C^2W (Command and Control Warfare) in its military application, cannot be a separate action in itself. For instance, it cannot provide a military presence or hold ground, but in fact, it is an integral part to existing and future architecture. C^2W incorporates the use of operational security, military deception, psychological operations, electronic warfare, and physical destruction, all supported by intelligence, to destroy the adversary's ability to wage war while protecting ours. It has

defensive and offensive aspects as well as lethal and non-lethal components.[3] Colonel Campen sums it up best concerning an offensive or defensive approach to IW, "the nation that expects to wage and to win at information war must strike just the right balance between its offensive and defensive capabilities. If it cannot, it risks the paradox of fielding a superbly equipped offensive force that also is the most vulnerable to the tools and tactics of IW."[4]

Defense

This revolution could put at risk high-value national assets outside the traditional battlefield and theater of "over there" power projection in a way that affects national military strategy and broader US national security strategy.[5] An adversary will likely not have the complex array of information systems the US has, but this will not deter their capability to use relatively simple and inexpensive technology in covert ways against US unclassified systems.[6] Although a strong or active defense could be the precursor to developing a corresponding offense, it does not appear to have priority. This is despite a *Joint Security Commission Study* stating an imperative exists for the defense and intelligence communities to focus more attention on information security. Security policies realistically must match IW threats.[7] Whatever IW strategy can do for the US can be used by enemies against the US. Therefore, systems must be made robust and have "electronic survivability." The US can do this by taking advantage of all national assets and using all its vast society's capabilities, especially the civil government and business sectors.[8]

The military and its supporting agencies are just as vulnerable at the operational and tactical levels. "As we learned in DESERT STORM, about 98 percent of the sorts of things comm-wise that we pass to conduct business on a day-to-day basis—like logistics, financial information, pay statements, medical—all goes on unclassified, commercial long-haul comms," according to Colonel Frank Morgan, commander of the Air Force Information Warfare Center (AFIWC). "We have not traditionally provided security for non-DOD or non-military comm bands."[9]

At least 122 nations have computer espionage programs, and the computer underground considers the Defense Department "easy pickings." Reported computer break-ins are expanding by more than 152 percent a year.[10] ID needs to begin at home. Defense must focus on confounding the challenger's search for acceptable alternatives to force-on-force (an adversary will use technical, tactical, and operational innovations to reduce risk, ideally to zero) by developing a response that guarantees the challenger unacceptable costs if they initiate an offensive challenge.[11] The US and its military should not put more money and effort into offensive, information-based weapons, when it cannot protect its own national systems.

Offense

Information-based systems will play a critical role in future conflict. Cyberspace will be another medium of conflict and the prize of victory will be ID.[12] Offensive systems will seek "electronic decapitation" of the enemy's abilities to command and control by virtually blinding him.[13] These measures will realistically save lives and shorten battles. On the national level, political, moral, and practical sensitivities may discourage making war

directly upon leaders, people, or their infrastructure; but there are links to other key systemic elements. A practical approach is to employ ID against an enemy's centers of gravity.[14] Strategic information systems in states with high technomic capability oftentimes are mirrored by operational-level systems of equal complexity, and all are vulnerable to attack.[15]

While emphasis should be on defensive measures, future wars will include information campaigns. An adversary's information flow must be specifically targeted and ID achieved. A new paradigm, "shock warfare," based not on attrition, but on the ability to paralyze and shock the enemy, will force him to follow a desired course. The war may begin with information suppression operations focused at reducing the enemy's battlefield awareness.[16] This will attempt to affect their operational planning, force deployment, sustainment of forces, and redeployment, much the same way we would expect them to do.[17] Former US Army Chief of Staff, General Gordon Sullivan, says connectivity is the key and the 21st century Army will direct its attention toward the lines that connect the boxes [horizontal and vertical lines of communications].[18]

The US Army's *"Force XXI"* project is an excellent example of the military's concern and its efforts to gain ID on the future battlefield. ID will be accomplished through digitization of the battlefield, defined by Brigadier General Joseph Oder, director of the Digitization Special Task Force, as "the application of information technologies to acquire, exchange, and employ timely digital information throughout the battlespace..." In such an environment, ID truly becomes the "arena of great contest" for it means that knowledge advantage about location could prove decisive, given the precision and destructive potential of modern weaponry.[19]

ID whether defensive or offensive in nature, is driving the impetus for future development of military strategy from the strategic to tactical levels. With a constrained budget and aging infrastructure, critical decisions will have to be made on where to channel the billions of dollars it will take to continue our leadership in information-based technologies and their subsequent uses in warfare.

Notes

[1] Office of the White House, *A National Security Strategy of Engagement and Enlargement*, February 1996, 24

[2] John I. Alger, "Declaring Information War," *Jane's International Defense Review* 29 (July 1996): 54.

[3] Major General Kenneth A. Minihan, "Information Dominance, Winning in the New Dimension of Warfare," *Spokesman* 34 (October 1994): 12.

[4] Colonel Alan D. Campen, "Rush to Information-Based Warfare Gambles with National Security," *Signal* 49, no. 11 (July 1995): 69.

[5] Roger C. Molander and others. "Strategic Information Warfare: A New Face of War," *Parameters* 26, no. 3 (Autumn 1996): 83.

[6]Admiral James B. Busey IV, "Information Warfare Calculus Mandates Protective Actions," *Signal* 49 (October 1994): 15.

[7] Clarence A. Robinson, Jr., "Crucial Network Imperatives Spawn Information War Peril," *Signal* 50, no. 10 (June 1996):35-36.

[8] Colonel Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal* 8, no. 4 (Winter 1994): 39

[9] Stephen M. Hardy, "The New Guerrilla Warfare," *Journal of Electronic Defense* 19, no. 9 (September 1996): 48.

[10] Clarence A. Robinson, Jr., "Defense Organizations Safeguards War Fighters' Information Flow," *Signal* 50, no. 2 (October 1995): 15.

[11] Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (Autumn 1996): 98.

[12] Major General Kenneth A. Minihan, "Information Dominance: Meeting the Intelligence Needs of the 21st Century," *American Intelligence Journal* 15 (Spring/Summer 1994): 18.

[13] Jensen, 37.

[14] John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review*, Summer 1994, 28.

[15] Colonel Richard Szafranski, "A Theory of Information Warfare," *Airpower Journal* 9, no. 1 (Spring 1995): 62.

[16] Thomas G. Mahnken, "War in the Information Age," *Joint Force Quarterly*: *JFQ* 10 (Winter 1995-96): 40-41.

Notes

[17] Lieutenant General James R. Clapper, Jr., and LTC Eben H. Trevino, Jr., "Critical Security Dominates Information Warfare Moves," *Signal* 49, no. 7 (March 1995): 72.

[18] Harknett, 101.

[19] Ibid., 94.

Chapter 3

What Will It Cost?

The tools of information war are well known, cheap and ubiquitous and unlikely to be monopolized by any side.

—Martin van Creveld

Cyberspace is a free flowing zone to which anyone has access, if they have a minimal level of capital...and we had better be prepared for zones of creativity in our opponents we've never dreamed of.

—House Speaker Newt Gingrich (R-GA)
AFCEA Conference

What ID will cost cannot be equated to dollar figures alone. The ability to ascertain actual budgetary cost is nebulous at best. The real question may lie in understanding existing vulnerabilities and the cost of protecting systems.

Budget

With time honored precepts of warfare being challenged by information-intensive combat systems, leaders must decide if sophisticated electronic warfare tools can be effective, not only against a major threat, but against the more likely low-technology adversaries, fanatics, or rogue nations not dependent on free-following information.[1] There is another reason for a coherent ID strategy, carefully considered, tested, tried, and prudently implemented. The wrong path may cost more than the US is willing to bear.

It is difficult to find information on the actual monetary cost of national and military information-based infrastructure. IW currently costs the United States an estimated $100-300 billion per year, and the financial impact on the US economy increases every year.[2] "Black budget" programs, for which dollar amounts are secret, reportedly could grow to more than $1 billion over the next several years.[3] The latest technology is a fast moving target and paying for it may the toughest problem of all for the military and non-military sectors. Military leaders say they are already $20 billion short of what they need just for routine modernization.[4] Over 9.5 percent ($23 billion) of the Fiscal Year 1997 defense budget was submitted for command, control, communications and computers. This was down only slightly from the previous years, but well above other programs that were severely cut.[5]

There is not enough funding to support even the security needs of existing systems. The Assistant Secretary of Defense for C3I, Emmett Paige, Jr., says adequate and reasonable expenditures are being made, but if available, an additional $2 billion could be applied immediately to older DOD systems. He maintains even more will be needed to protect systems across the entire government.[6] Lieutenant General Otto J. Guenther, USA, the director of Information Systems for C4, is heavily involved in the Army's "C2 Protect" training. He says communications and computer security areas are currently under-funded or, in the case of security training, not funded at all. In 1994 and 1995, there was a 76 percent reduction in funding for security system's research, development, and test and evaluation, while reliance on these systems increased dramatically.[7]

The US is the world's most interconnected country,[8] and the information security problem is worsening as the number of computers in the government is increasing.

Reliance on these systems leaves the US vulnerable to attack, and if attacks come, they may come in advance of any formal declaration of hostile intent. Attacks will be against leader's knowledge and belief systems, aimed at influencing their choices, and in the future, even non-combatants will be targets.[9]

Initial efforts by the Clinton administration to craft a "politically correct" role for the federal government in securing the national information infrastructure was censored by those concerned over intellectual property and privacy issues. These concerns, though legitimate in a open market system, override the more pressing issues of national security.[10] A conservative estimate is that more than 90 percent of defense networks use commercial systems (more than 95 percent of the defense and intelligence community voice and data traffic uses the public telephone system).[11] The vulnerability of these systems require immediate action. The military approaches exercises and planning for military operations with communications systems running at 100 percent and untouchable, but the loss of these networks is anticipated (enemies could simply deny us information by tampering with our links). A commander may understand human systems, but if they don't understand the automated systems on the battlefield of 2015, they will be vulnerable to surprise and possibly defeat.[12]

Major General Thomas L. Wilkerson, USMC, commanding general, Marine Forces Reserve, told a group at the Armed Forces Communications and Electronics Association Western Conference in January 1996, "the enemy has a disturbing habit of not listening to the lecture. We set up the rules, they don't follow the rules. Our systems have to be adaptable enough that, when the enemy doesn't follow the rules, we still prevail. We may be more vulnerable than we are threatening."[13]

Finally, a Joint Security Commission study said an imperative exists for the defense and intelligence communities to focus more attention on information security. The report further emphasized the identity of everyone with access to networks to which US systems are connected can no longer be known with assurance.[14] Our vulnerabilities are compounded by the confusion and disagreement between the military and commercial sectors over standards and responsibility for security measures. Senator Robert Kerry says the information infrastructure vulnerability extends beyond the concept of an Achilles heel. "I would liken it to a carotid artery where the nation could bleed to death if the financial system or power grid were shut down."[15] The US cannot avoid putting more emphasis on the defense of information systems.

Notes

[1] Colonel Alan D. Campen, "Information Warfare is Rife with Promise, Peril," *Signal* 48 (November 1993): 19.

[2] Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1994), 16.

[3] Steven Aftergood, "The Soft-Kill Fallacy," *The Bulletin of the Atomic Scientists* 50 (September/October 1994): 40.

[4] Richard J. Newman, "Warfare 2020," *US News and World Report*, August 5, 1996, 40.

[5] Robert Ropelewski, "Command, Control Priorities Shift, Steady Funding Persists," *Signal* 50, no. 9 (May 1996): 41.

[6] Clarence A. Robinson, Jr., "Information Warfare Strings Trip Wire Warning Strategy," *Signal* 50, no. 9 (May 1996): 29.

[7] Clarence A. Robinson, Jr., "Army Information Operations Protect Command and Control," *Signal* 50, no. 11 (July 1996): 49.

[8] Clarence A. Robinson, Jr., "Defense Organization Safeguards War Fighters' Information Flow," *Signal* 50, no. 2 (October 1995): 18.

[9] Colonel Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995): 64.

[10] Colonel Alan D. Campen, "Vulnerability of Info Systems Demands Immediate Action," *National Defense* 80, no. 512 (November 1995): 26-27.

[11] Clarence A. Robinson, Jr., "Crucial Network Imperatives Spawn Information War Peril," *Signal* 50, no. 10 (June 1996): 35.

Notes

[12] Commander George F. Kraus, Jr., "Information Warfare in 2015," *Proceedings* 121, no. 8 (August 1995): 44.

[13] Beverly P. Mowery, "Information Determines the Battlespace as World Changes Camouflage Threats," *Signal* 50, no. 8, (April 1996): 68.

[14] Robinson, 35.

[15] Robert K. Ackerman, "Commercial, Military Information Security Requirements Meld," *Signal* 50, no. 9 (May 1996): 108.

Chapter 4

Who Are Our Future Adversaries?

> *The more sophisticated and expensive the information gathering system, the greater the premium opponents will put on disabling it....The pay-off for shooting down a state-of-the-art radar surveillance aircraft, for example, will surely attract efforts to do so.*
>
> —Gulf War Air-Power Summary Report

The majority of crises for the foreseeable future will involve second- and third-world countries. Since most of the countries with first world status are either US allies, at relative peace, or rebuilding. So America's physical borders will likely not be threatened directly. Greatest threats will come from espionage, subversive terrorists groups, gangs, fanatics, and cyber-warriors. But the results could be just as disastrous as force on force; with certain disruption of economic, political, social, or physical infrastructure.

The US dependence on technology will create vulnerabilities our enemies will not hesitate to exploit now and in the future. Martin Libicki of the Center for Advanced Concepts and Technology at the National Defense University reports that every passing week the US appears to grow more vulnerable to attacks on its soft underbelly—its national information infrastructure. "It must be assumed that any nation at war with the United States will attack military systems (especially logistics and mobilization systems) any way it can..."[1] Since, only 25 percent of the planet can be considered developed, there are billions of "Have-Not" inhabitants. Because of the Global Network the Have-

Nots receive visual images of the more fortunate "Haves." "Through CNN, Dynasty, upscale sitcoms, and global programming, the Have-Nots see for themselves how 'the other half' live, and they want their share of the pie. When there's nothing to lose, there's nothing to fear."[2]

It has always been good tactics for an army to attack an adversary's command and control, but the US, until now, has not been particularly vulnerable to outside attack. As stated above, it is clear almost any enemy will try to degrade the US information systems.[3] This may be their only course of action and a retaliatory response using the military might not be feasible. Future wars will likely not resemble the Gulf War anyway. The freedom to militarily attack an opponent may be unlikely, especially in response to cyber attacks which are difficult to detect and identify. Concern over potential international response (Chinese, Soviet, UN) will probably restrict retaliation methods. Information attacks are difficult to track even with present capabilities and, it will be even tougher to prove responsibility. The enemy understands our reluctance and will use it as his sanctuary to operate from with impunity.[4]

While the US understands the motives, what about the means? Estimates by the National Security Agency (NSA) are that more than 120 nations established IW cadres to take advantage of their adversary's operational security weaknesses.[5] These are potential IW armies ready to take advantage of US vulnerabilities. Experts note no nation, at least for the foreseeable future, will try to take on the US military in a battle of attrition, but the greatest threats in the near term (10-20 years) will be second- and third-world countries using unconventional means. It makes sense to put the preponderance of our scarce resources into an active defense against the most likely threats.

Notes

[1] Martin C. Libicki, P*rotecting the United States in Cyberspace* (Washington DC: Institute for National Strategic Studies), 1, 12.

[2] Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1994), 21.

[3] Commander George F. Kraus, Jr., "Information Warfare in 2015," *Proceedings* 121, no. 8 (August 1995): 42.

[4] Thomas G. Mahnken, "War in the Information Age," *Joint Force Quarterly*: *JFQ* 10 (Winter 1995-96): 43.

[5] Stephen M. Hardy, "The New Guerrilla Warfare," *Journal of Electronic Defense* 19, no. 9 (September 1996): 50.

Chapter 5

Conclusion

The information technology explosion has led to a flurry of books and reports on IW, and its multi-faceted subsets (i.e., information dominance). Its overwhelming appeal, as a cure for the diminishing budget and resource constraints, fuels US desires to embrace its healing powers. But the US is giving in too quickly, willing to sacrifice present strengths for the promise of an uncertain future. The US should take time to formulate a coherent IW strategy, restructure to accommodate information technology tools, and prepare in earnest for the 21st century. The greatest single mistake faced by all the Services is to yield to the usual temptation of adopting new technologies as merely force multipliers for the current way they do business: to make information technologies of IW fit familiar models.[1] It would be a mistake to try and fight tomorrow's battles with yesterday's strategies.

It is not proposed the US become complacent, just the opposite. Information technology provides an opportunity for forces to do more with less. Nations are not turning their backs on the potential afforded by this "revolution." In fact, the Russians have shifted to smaller, highly mobile, and well-informed forces.[2] Failure to develop a strategy for offensive and defensive IW could put the US on the receiving end of an "electronic Pearl Harbor."[3] The ability to disrupt enemy information networks may deter

aggression and gives credence to continued offensive development capability. ID could be obtained by intensive research and development associated with an active defensive posture. An active defense would protect our national infrastructure, create a strong deterrence, and provide time for measuring and developing offensive abilities for operational and tactical employment against future major threats.

Lessons learned from the Gulf War may be misleading and the next wars will most likely be under vastly different circumstances, with worthy opponents in closer quarters. To avoid blind alleys, it is more important to use this period of relative calm (no major threats to our own borders) to demonstrate and validate new concepts, instead of going ahead with full-scale development. We need better forecasts of the rapidly changing world situation. According to John M. Collins, senior specialist in national defense with the Library of Congress, "basic research should receive higher priority now."[4]

So Why Slow Down?

How technologies might unfold and how they might be used must be understood not only in our own strategies, but in the rest of the world's nation and non-nation state powers. Strategy and doctrine take time to develop and validate. In the meantime, the US needs a national definition, strategy, and coordinating mechanism for IW, an azimuth for a coordinated effort from the strategic to the tactical level.[5] "The changes necessary to exploit the potential of ID go well beyond the technologies themselves...simply grafting new technology onto existing structures, will have negative effects."[6]

Maybe a greater danger is that little attention is paid to offensive information actions against the US forces in simulations: they are just assumed away. There are no useful

measures of the relative combat value of intelligence, communications, deception, or other information-warfare applications existing in simulations, models, or games. Practically none of the simulations address operational or strategic level vulnerabilities.[7] The military is just as guilty of exercising IW the same way it has communications networks in field exercises (communication backbones are kept in place to let combat units train and maneuver, seldom destroyed).

History is full of examples to remind us that better technology is not always triumphant. In Bosnia, a heavy military presence appears to be the key to success and still needed are "boots on the ground." General Reimer, Army Chief of Staff, thinks that even though soldiers will be equipped with advanced weapons and communications gear, "warfare will basically be the same" in 10 to 15 years. The Army is ever wary of the Viet Cong-like foe, who can defeat technology with rudimentary tactics and a willingness to sacrifice lives.[8] Future adversaries, a fearsome new breed of the post-Cold War, are not stamped in the Western mold and have few strategic centers of gravity. That enemy must be better understood.

The Armed Forces must rethink manpower issues and organizational design policies now, to ensure there is no mismatch between soldier capabilities and the intellectual demands imposed by the technology and systems now being designed. The Army will need to draw increasingly upon the college-educated rather than high school graduates, which places the Army in direct competition with the private sector, drawing from the same manpower pool.[9] Conferences, like the *Army 2010 Conference*, highlight the need to understand the soldier requirements. This all takes time. Even with implementation taking place today, the system cannot turn over that fast. The way the US and military

organize and use technology will be critical. We constantly hear of data overload, but again propose to increase information flow.

Almost anyone can participate in the high tech world (of course, at varying degrees). Broad assessments must categorize potential opponents by their potential vulnerability to "information attacks." This should be one of the prerequisites to determine how much effort should be placed on an effective offensive or defensive deterrence. The new kinds of weapons (viruses, microwave weapons) need to be subjected to the same kind of analytic scrutiny as other weapon systems. What kind of enemies will offensive (information) warfare be leveled against?[10]

Another reason to test US resolve is that political and legal issues surrounding information war are murky at best.[11] The United States is an open society, making it far more likely to get a "bruised lip" in a cyberwar. How does IW fit into the realm of "armed conflict?" It will take time to determine the exact application of traditional principles to IW situations. The US needs understandable principles to actually employ IW in specific scenarios. Old concepts and theories of defense and offense do not necessarily apply to IW, although there are attempts to make the "square peg fit the round hole."

Bruce W. McConnell, chief of information policy and technology at the White House Office of Management and Budget, suggested that establishing effective defensive IW depends on convincing the private sector of its importance.[12] This is a challenging task. Even Defense Secretary Perry stated, "Commanders are revising their doctrine and tactics to take advantage of this technology, and they want to pull it faster into their war planning. The key technology they want is information technology, and it is being developed at a breathtaking pace, but not by the Defense Department...it is being

developed by commercial computer, dual-use technology firms, and small high-technology businesses and universities. The department cannot pull this technology from these sources without acquisition reform..."[13]

Reasons to slow down are too numerous to compile. But consider there are still no adequate warning systems for distinguishing between strategic IW attacks and other kinds of cyberspace activity. There is increased pressure to form coalitions (Gulf War, Bosnia, Somalia, etc.) which will likely increase the vulnerabilities of the security postures of all the partners to strategic IW attack.[14] And the list goes on.

Solutions?

We have only touched the tip of the iceberg regarding IW and its subsets. Proposed solutions are as varied and different as the names for information-based warfare. National agencies, the DOD, and each of the Services, from the highest to lowest levels, are dealing earnestly with this "revolution." The evidence exists in the mountains of material being written on the subject from proposals to doctrine development. But the military must take its time, slow down the drawdown, develop strategy and doctrine, reform the acquisition system, and embrace the new technology. Time must be taken to determine if IW is a fad or the ultimate weapon. The following suggestions are a few possible approaches to strategy and doctrine development for IW to ultimately achieve ID:

•As information-warfare concepts and the associated systems and techniques move into the US force structure, gaming should change to reflect the new approach and threats.[15]

•One course of action is to develop a dual track program. (1) Defensive—ensure the vulnerabilities of systems are identified and safeguards implemented, and (2) Offensive—develop an offensive information-based system which can and will respond to enemy probes, and assures ID on the battlefield.[16]

•The rapid diffusion of information challenges the relevance of traditional hierarchical organizations. This can create a dilemma in the form of a commander's choice of locating forward with the soldiers or in the command post.[17] This is not new in itself, but if a division commander can see what the soldier sees, will he be tempted to make the decisions? The situational dynamics must be tested in all Services as is being done in *Force XXI.*

•Reduce the centralization of databases to minimize their overall vulnerability to disruption, destruction, corruption, or other forms of compromise. This will not be easy in view of the need to share common databases.[18]

•The US must develop a coherent national-level policy on the military and strategic use of new IW technologies. The Joint Chiefs have introduced an excellent start through their brochure, *Information Warfare, A Strategy for Peace...The Decisive Edge in War.* This brochure gives a common framework for the services outlining IW concepts and ongoing initiatives that will help determine future strategy.[19]

•Doctrine, organizational structures, and procedures have to be revamped to ensure the speedy flow of information from sensor to shooter.

•IW defenses must be capable of detecting who enters secure data bases and the invader must be convicted based on supportable evidence. This will require changes to

national and international laws. Conventions on IW must begin immediately if the Chemical Warfare Convention is an indicator of the span and complexity of the subject.

•Establish rules of engagement for employing IW. This will be a difficult task when the parameters of IW are not defined and it has not been declared a legitimate weapon.

•The military must avoid C^3 standardization and seek multiple, different but inter-operable systems so that a "golden BB" can't take its systems down.[20]

•The vulnerability of the "home" information resources and the potential for a dramatic shift in the traditional conflict environment, demand everyone gets the right degree of training.[21]

•All services must form protection systems, like the Army's *C^2 Protect*, against potential threats to address all of the protection schemes from the national command authorities to the foxhole, or the cockpit, or the ship.[22]

•If the US is convinced information-based warfare is not a fad or trend pushed by those who stand to gain from defense dollars, as suggested by the *Secretary of Defense Strategic Studies Group*, the development of an integrated command and control architecture should be done first, followed by the weapon systems designed to operate with the command and control framework.[23]

The present environment suggests the public wants a smaller, more efficient force to serve the nation's needs. It must be done with a reduced force structure and a constrained budget. Almost all futurists agree, the future threats will not diminish, but actually increase with less defined borders and intent. The US must design a force that combines an intellectual framework with the nation's policy, yet vulnerabilities must be defended. Can resources currently committed to systems that will ultimately be eliminated be

reduced in order to grasp knowledge-based warfare more quickly, or is this a risky strategy, giving up awesome capabilities on a bet IW can be fully developed before we face a worthy opponent?[24] Also, there is no leadership in this area.

While Services are making valiant strides, recognizing the inevitable—"do more with less," there is no consensus about which government agency should lead. There are only hints of top-level guidance that must pilot this unprecedented shift of international security policy; rules of engagement will have to come from the top. IW will have to be brought into balance to go with the weapons that will be used for at least the next 20 years.[25]

The US has ID today, is the world's leader in information technology and has the world's best military. The US has the time, research and development experience, and motivation to take its military into the 21st century. It can accomplish ID offensively and defensively by first instituting a strategic active, free-flowing defense that will protect its own systems and serve as a deterrence. This effort can be accelerated through a coherent national strategy, and subsequent national military strategy, that provides a framework upon which to build. The US must not get caught up in the IW hype and put military men and women at risk in the near term, but plan for a successful IW future.

Notes

[1] George J. Stein, "Information Warfare," *Airpower Journal* 9, no. 1 (Spring 1995): 1.

[2] John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review*, Summer 1994, 30.

[3] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston, Mass.: Little, Brown and Co., 1993), 149.

[4] George F. Watson, ed., "The Challenge of Post-Gulf Conflicts," *IEEE Spectrum*, September 1991, 56.

[5] Lieutenant General James R. Clapper, Jr., and LTC Eben H. Trevino, Jr., "Critical Security Dominates Information Warfare Moves," *Signal* 49, no. 7 (March 1995): 71.

Notes

[6] John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review,* Summer 1994, 29.

[7] Commander George F. Kraus, Jr., "Information Warfare in 2015," *Proceedings* 121, no. 8 (August 1995): 44.

[8] Richard J. Newman, "Warfare 2020," *US News and World Report*, August 5, 1996, 37-40.

[9] Major E. Casey Wardynski, "The Labor Economics of Information Warfare," *Military Review* 75, no. 3 (May-June 1995): 56-58.

[10] Glen Buchan, "Information War and the Air Force: Wave of the Future? Current Fad?, *Project Air Force-Issue Paper*, (RAND), March 1996, 9. (www.RAND.org/publications/IP/IP149/index.html)

[11] George J. Stein, *Battlefield of the Future*, (chapter 6, Information War-Cyberwar-Netwar) [www.cdsr.af.mil/battle/chp6.html], 6,7.

[12] Robert K. Ackerman, "Commercial, Military Information Security Requirements Meld," *Signal*, May 1996, 109.

[13] Robert Ropelewski, "Command, Control Priorities Shift, Steady Funding Persists," *Signal*, May 1996, 44.

[14] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," *Parameters*, Autumn 1996, 86 (reprinted from RAND, 1996).

[15] Commander George F. Kraus, Jr., Navy (retired), "Information Warfare in 2015," *Proceedings*, August 1995, 45.

[16] Donald E. Ryan, Jr., "Implications of Information-Based Warfare," *Joint Force Quarterly: JFQ*, Autumn/Winter 1994-95, 116.

[17] General Frederick M. Franks, Jr., "Winning the Information War: Evolution and Revolution," address to the Association of the US Army Symposium, Orlando, Florida, 8 February 1994.

[18] Glenn Buchan, *Information War and the Air Force: Wave of the Future? Current Fad?*, RAND Issue Paper 149 (Santa Monica, Calif.: RAND, March 1996), 10 n.p.; on-line, Internet, 14 February 1997, available from http://www.RAND.org// publications/IP/IP149/ index.html.

[19] Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace...The Decisive Edge in War.*

[20] Colonel Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal* 8, no. 4 (Winter 1994): 40.

[21] John I. Alger, "Declaring Information War, Early Training Crucial to Awareness," *Jane's International Defense Review* 29 (July 1996): 54.

[22] Clarence A. Robinson, Jr., "Army Information Operations Protect Command and Control," *Signal* 50, no. 11 (July 1996): 47.

[23] Lawrence E. Casper and others., "Knowledge-Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly*: *JFQ* 13 (Autumn 1996): 84.

[24] Admiral William A. Owens, "The Emerging System of Systems," *Proceedings* 121, no. 5 (May 1995): 36-39.

Notes

[25] Colonel Alan D. Campen, "Assessments Necessary in Coming to Terms with Information War," *Signal* 50, no. 10 (June 1996): 47-49.

Bibliography

Ackerman, Robert K. "Commercial, Military Information Security Requirements Meld." *Signal* 50, no. 9 (May 1996): 108-109.

Ackerman, Robert K. "Marine Corps Information Warfare Combines Services' Needs, Defines Their Differences." *Signal* 50, no. 11 (July 1996): 61-65.

Ackerman, Robert K. "Military Planners Gird for Information Revolution." *Signal* 49, no. 9 (May 1995): 71-76.

Ackerman, Robert K. "Navy Doctrine, Systems Face Information Warfare Makeover." *Signal* 50, no. 11 (July 1996): 57-60.

Adam, John A. "Warfare in the Information Age." *IEEE Spectrum* 28 (September 1991): 26-33.

Aftergood, Steven. "The Soft-Kill Fallacy." *The Bulletin of the Atomic Scientist* 50 (September-October 1994): 40-45.

Alger, John I. "Declaring Information War: Early Training Crucial to Awareness." *Jane's International Defense* 29 (July 1996): 54-55.

Arquilla, John. "The Strategic Implications of Information Dominance." *Strategic Review*, Summer 1994, 24-30.

Arquilla, John and David Ronfeldt. *Cyberwar is Coming*. RAND Report P-7791. Santa Monica, Calif., 1992.

Blazar, Ernest. "Planners: Information is the Best Weapon." *Navy Times* 43 (September 5, 1994).

Boorda, Jeremy M. "Leading the Revolution in C^4I." *Joint Force Quarterly: JFQ* 9 (Autumn 1995): 14-17.

Braunberg, Andrew C. "Air Force Pursues Two-Sided Information Warfare Strategy." *Signal* 50, no. 11 (July 1996): 63-65.

Buchan, Glenn. *Information War and the Air Force: Wave of the Future? Current Fad?* RAND Issue Paper 149. Santa Monica, Calif., March 1996, n. p. On-line. Internet, 14 February 1997. Available from http://www.RAND.org/publications/ip/ip149/index.html.

Busey, Admiral James B. "Information Warfare Calculus Mandates Protective Actions." *Signal* 49 (October 1994): 15.

Campen, Colonel Alan D. "Vulnerability of Info Systems Demands Immediate Action." *National Defense* 80, no. 512 (November 1995): 26-27.

Campen, Colonel Alan D. "Assessments Necessary in Coming to Terms with Information War." *Signal* 50, no. 10 (June 1996): 47-49.

Campen, Colonel Alan D. "Information Warfare is Rife with Promise, Peril." *Signal* 48 (November 1993): 19-20.

Campen, Colonel Alan D. "Rush to Information-Based Warfare Gambles with National Society." *Signal* 49, no. 11 (July 1995): 67-69.

Casper, Lawrence E., et. al. "Knowledge-Based Warfare: A Security Strategy for the Next Century." *Joint Force Quarterly: JFQ* 13 (Autumn 1996): 81-89.

Clapper, Lieutenant General James R., Jr. and Eben H. Trevino, Jr. "Critical Security Dominates Information Warfare Moves." *Signal* 49, no. 7 (March 1995): 71-72.

DiNardo, R. L. and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." *Airpower Journal* 9, no. 4 (Winter 1995): 69-79.

Franks, General Frederick M. "Winning the Information War." Address. Association of the US Army Symposium, Orlando, Florida, 8 February 1994. (can be found in *Vital Speeches of the Day*).

Gehly, Darrly. "Controlling the Battlefield." *Journal of Electronic Defense* 16 (June 1993): 42-49.

Hardy, Stephen M. "The New Guerrilla Warfare." *Journal of Electronic Defense* 19, no. 9 (September 1996): 46-52.

Harkett, Richard. "Information Warfare and Deterrence." *Parameters* 26, no. 3 (Autumn 1996): 93-107.

Jensen, Colonel Owen E. "Information Warfare: Principles of Third-Wave War." *Airpower Journal* 8, no. 4 (Winter 1994): 35-43.

Joint Chiefs of Staff. *C4I for the Warrior: A 1995 Progress Report.*, 1995.

Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace....The Decisive Edge in War.*

Joint Chiefs of Staff. *Joint Vision 2010.*

Kitfield, James. "Fit To Fight." *National Journal* 28, no. 11 (March 16, 1996): 582.

Kraft, Michael. *Technology and Politics*. Durham and London: Duke University Press, 1988.

Kraus, Commander George R. "Information Warfare in 2015." *US Naval Institute Proceedings* 121, no. 8 (August 1995): 42-45.

Libicki, Martin. "Protecting the United States in Cyberspace." Washington: National Defense University, Institute for National Strategic Studies.

Mahnken, Thomas G. "War in the Information Age." *Joint Force Quarterly: JFQ* 10 (Winter 1995-1996): 39-43.

Mann, Colonel Edward. "Desert Storm—The First Information War?" *Airpower Journal*, Winter 1994, 5-14.

Matthews, William. "Susceptible to Sabotage." *Air Force Times* 56, no. 27 (February 5, 1996): 28.

Minihan, Major General Kenneth A. "Information Dominance: Meeting the Intelligence Needs of the 21st Century." *American Intelligence Journal* 15 (Spring/Summer 1994): 15-19.

Minihan, Major General Kenneth A. "Information Dominance, Winning in the New Dimension of Warfare." *Spokesman* 34 (October 1994): 10-12.

Molander, Roger C. et. al., "Strategic Information Warfare: A New Face of War." *Parameters* 26, no. 3 (Autumn 1996): 81-92. (original source RAND Report MR-661-OSD, 1996).

Morris, Chris, et. al., "Weapons of Mass Protection." *Airpower Journal* 9, no. 1 (Spring 1995): 15-29.

Mowery, Beverly P. "Information Determines the Battlespace as World Changes Camouflage." *Signal* 50, no. 8 (April 1996): 65-69.

Newman, Richard J. "Warfare 2020." *US News & World Report*, August 5, 1996, 34-43.

Office of the White House. *A National Security Strategy of Engagement and Enlargement*. February 1996.

Owens, Admiral William A. "The Emerging System of Systems." *US Naval Institute Proceedings* 121, no. 5 (May 1995):35-39.

Petersen, John H. "Info Wars." *US Naval Institute Proceedings* 119 (May 1993): 85-92.

Petersen, John L. *Road to 2012*. Corte Madera, Calif.: Waite Group Press, 1994.

Riccardelli, Colonel Richard F. "The Information and Intelligence Revolution." *Military Review* 75, no. 5 (September-October 1995): 82-87.

Robinson, Clarence A. "Army Information Operations Protect Command and Control." *Signal* 50, no. 11 (July 1996): 47-50.

Robinson, Clarence A. "Crucial Network Imperatives Spawn Information War Peril." *Signal* 50, no. 10 (June 1996): 35-38.

Robinson, Clarence A. "Defense Organizations Safeguards War Fighters' Information Flow." *Signal* 50, no. 2 (October 1995): 15-16.

Robinson, Clarence A. "Digital Intelligence Extends Army Force Projection Power." *Signal,* August 1994, 33-35.

Robinson, Clarence A. "Information Warfare Strings Trip Wire Warning Strategy." *Signal* 50, no. 9 (May 1996): 29-33.

Robinson, Clarence A. "Modern Battlefield Demand Stalwart Industry Practices." *Signal* 50, no. 8 (April 1996): 43-46.

Robinson, Clarence A. "Rapid Technology Growth Spawns Land Information Warfare Activity." *Signal*, July 1996, 51-54.

Robinson, Clarence A. "Redundancy, Robustness Protect Vital National Information Links." *Signal* 50, no. 9 (May 1996): 36-39.

Ropelewski, Robert. "Command, Control Priorities Shift, Steady Funding Persists." *Signal* 50, no. 9 (May 1996): 41-44.

Ryan, Lieutenant Colonel Donald E., Jr. "Implications of Information-Based Warfare." *Joint Force Quarterly: JFQ* 6 (Autumn-Winter 1994-1995): 114-116.

Schwartau, Winn. *Information Warfare*. New York: Thunder's Mouth Press, 1994.

Stein, George J. "Information War - Cyberwar—Netwar." *In Battlefield of the Future: 21st Century Warfare Issues*. Edited by Barry R. Schneider, and Lawrence E. Grinter, Maxwell AFB, Al.: Air University Press, September 1995. n. p. On-line. Internet. Available from: http://www.cdsar.af.mil/battle/chp6.html.

Stein, George. "Information Warfare." *Airpower Journal* 9, no. 1 (Spring 1995): 31-39.

Stewart, Major General John F. "Intelligence Strategy for the 21st Century." *Military Review* 75, no. 5 (September-October 1995): 75-81.

Szafranski, Colonel Richard. "A Theory of Information Warfare - Preparing for 2020." *Airpower Journal* 9, no. 1 (Spring 1995): 56-65.

Toffler, Alvin and Heidi. *War and Anti-War*. New York: Little, Brown and Company, 1993.

Wardynski, Major E. Casey. "The Labor Economics of Information Warfare." Military Review 75, no. 3 (May-June 1995): 56-61.

Watson, George F. "The Challenge of Post-Gulf Conflicts." IEEE Spectrum, September 1991, 53-57.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112