PUBLICATION

Information Superiority: What Is It? How to Achieve It?

Walter P. Fairbanks

June 1999

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Walter Fairbanks is currently the Deputy Director for Programs and Budget, Command, Control, Communications, and Computer Systems Directorate (J6), The Joint Staff, where he has served since 1992. Previous assignments, also in the field of communications-computers, have included the Office, Director of Information Systems for Command, Control, Communications, and Computers (ODISC^4), the U.S. Army Information Systems Command, and the Communications Systems Planning Element (CSPE), 7th Signal Brigade, U.S. Army, Europe. This report was prepared while he was a National Defense Fellow with the Program in 1997-98.

ISBN 1-879716-56-9 **P-99-4**

March 2000

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Ameritech
AT&T Corp.
Australian Telecommunications Users Group
Bell Atlantic
BellSouth Corp.
The Boeing Company
Booz-Allen & Hamilton, Inc.
Carvajal S.A. (Colombia)
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
CyberMedia Convergence Consulting
CyraCom International
DACOM (Korea)
ETRI (Korea)
eYak, Inc.
Fujitsu Research Institute (Japan)
GNB Technologies
Grupo Clarin (Argentina)
GTE Corp.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Intel Corp.
Kavner & Associates
Korea Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Eli Lilly and Co.
Lucent Technologies
John and Mary R. Markle Foundation
McCann North America
MediaOne Group
Merck & Co., Inc.
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
NEST−Boston
Nippon Telegraph & Telephone Corp. (Japan)
NMC/Northwestern University
Qwest Communications International, Inc.
Research Institute of Telecommunications and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
SK Telecom Co. Ltd. (Korea)
Strategy Assistance Services
TRW, Inc.
United States Government:
  Department of Commerce
    National Telecommunications and Information Administration
  Department of Defense
    Defense Intelligence Agency
    National Defense University
  Department of Health and Human Services
    National Library of Medicine
  Department of the Treasury
    Office of the Comptroller of the Currency
  Federal Communications Commission
  National Security Agency
  United States Postal Service

Acknowledgements

The author gratefully acknowledges the following people who reviewed and commented critically on the draft version of this report. Without their consideration, input, and encouragement, this study could not have been completed:

Robert Abney
David S. Alberts
C. Kenneth Allard
Dean C. Allard
Henry Allen
Joseph P. Bassi
Alan D. Campen
Denis Clift
Victor A. DeMarines
Michael P. Finn
Max L. Gross
Walter Jajko
Martin C. Libicki
Wayne Mayfield
Arthur L. Money
William A. Owens
Marilyn A. Quagliotti
Mike Rozea
Frank M. Snyder

These reviewers and the Program's Affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

I would like to thank in particular Mike Rozea, who interrupted a vacation on Cape Cod to discuss with me an early draft of this report. Other people who read this report in one form or another and provided invaluable assistance include Ann Birdsall, Rick Caroll, Michael A. Curci, Troy Douglas, Martin L. Ernst, Bernard C. Forcier, David A. Garrison, John Hennigan, William G. Kraus, Ron Mathis, Dianne Northfield, John A. Rolando, and Melvin A. Wilson.

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the Department of Defense or any other government agency or department.

Contents

Acknowledgements i

Executive Summary vii

Chapter One Introduction to Information Superiority 1

1.1 Ambiguity 2

1.2 The Role of Information Superiority in *Joint Vision 2010* 5

1.3 Think Joint! 6

1.4 Experimentation 6

1.5 Organization of the Discussion 8

Chapter Two C^4ISR and Its Pivotal Role in the Information Age 13

2.1 Warfare in the Information Age 13

2.1.1 Network-Centric Warfare 14

2.1.2 Breaking Familiar Practices 15

2.1.3 Optimizing the Flow of Information 16

2.2 Other Factors and Consequences 17

2.3 Money, Optimism, and a New Operational Framework 18

2.4 Cautions, Wisdom, and Criticism 19

2.5 Expectations 23

Chapter Three Information Superiority: Capability, Ability, or Condition? 25

3.1 Information Superiority and the C^4IFTW Vision 25

3.2. The Uses of Information Superiority 28

3.3 Information Superiority: A Condition 31

Chapter Four The Information Domain 33

4.1 Information and the Chaos of War 33

4.2 Information Superiority in an Operational Context 34

4.2.1 Scale of Information Domain Conditions 35

4.3 Theory versus Practice 37

4.3.1 Moving from the Theoretical 37

Chapter Five Can Information Superiority Be Measured? 41

5.1 Urgent Fury 41

5.2 Desert Shield/Desert Storm 43

5.3 Determining Information Superiority 45

Chapter Six From Vision to Reality: Achieving an Integrated C4ISR Capability Without Another Goldwater–Nichols Act 47

6.1 Information Superiority as an Objective of Joint Warfighting Capability 47

6.2 Opportunities for Improving C4ISR Modernization 48

6.2.1 The Joint Requirements Oversight Council (JROC) 50

6.2.2 Acquisition Categories 51

6.2.3 Management of Defense Acquisition Programs 52

6.2.4 Operational Requirements 53

6.3 Scenario 1: Increased Use of Executive Committees 54

6.3.1 Existing DOD Executive Committees 56

6.3.2 Advantages and Disadvantages of Executive Committees 57

6.4 Scenario 2: C4ISR Concept Exploration and Demonstration 58

6.4.1 Phase 0, Concept Exploration 58

6.4.2 Phase I, Program Definition 59

6.5 Joint C4ISR Concept Exploration and Demonstration Center 59

6.5.1 Existing Joint Organizations 60

6.5.2 Advantages and Disadvantages of a Joint C4ISR Concept Exploration and Demonstration Center 62

6.6 Combining the Two Scenarios 63

Chapter Seven Summary 65

Acronyms 67

Figures

2-1 Emerging Operational Concepts 20

3-1 "System of Systems": Dominating the Joint Battlespace 26

4-1 Scale of Information Domain Conditions 35

6-1 Defense Acquisition Phases and Milestones 53

6-2 Mission Need Statement Generation Process 54

Executive Summary

The amount of information commanders now need in order to conduct military operations has increased dramatically with the emergence of electronic information, leading to reliance on increasingly complex command, control, communications, computer and intelligence, surveillance, and reconnaissance (C^4ISR) systems. It has become fashionable to talk about achieving "information superiority" in the context of such new warfare concepts as network-centric warfare, knowledge-based warfare, command and control (C^2) warfare, information warfare, to name only a few of the trendiest. These concepts, and their underpinnings, derive from the information age and, in one form or another, subscribe to the notion of achieving information superiority. They do so, even though what information superiority means is often unclear and even though that term has been used to describe a variety of circumstances.

The report has three goals: first, to clarify what the term "information superiority" means and how information superiority can be achieved; second, to ascertain whether information superiority can be measured by assessing the performance of C^4ISR systems during military operations; and, third, to explore two scenarios for improving the Department of Defense's (DOD) approach to modernization of C^4ISR systems and enhancing interoperability.

The discussion is based on five premises: (1) that the DOD is committed to achieving information superiority; (2) that the C^4ISR portion of the overall DOD budget will not be increased; (3) that, for reasons of effectiveness and efficiency, joint and combined operations are embedded in the backbone of the U.S. military; (4) that the DOD desires to conduct future military operations by taking advantage of the synergism made possible by optimizing and blending the capabilities of each force component (ground, maritime, and air), thereby developing and using a multidimensional capability more powerful than any past joint force; and (5) that for a joint force to conduct synchronized military operations depends on the DOD's ability to employ and modernize protected, integrated, and interoperable C^4ISR systems.

Chapter One

Introduction to Information Superiority

Warriors have always sought to gain better information to reduce the uncertainties of war. In war decisions about whether to launch an offense or stay on the defense are based on information about the state of one's own forces, the state of the enemy's forces, the terrain, the climate, and so on.[1] To obtain information in the past commanders relied on books, maps, scouts, travelers, deserters, prisoners, diplomats, and spies. Other capabilities were developed and came into use, such as balloons and airplanes, as spotters—and the U.S. Air Force now teaches that in the use of those early airborne craft information superiority became "the first function of the Air Force."[2] With the emergence of the domain of electronic information, the amount of information commanders seek to conduct military operations increased dramatically,[3] leading them to rely on correspondingly increasingly complex command, control, communications, computer and intelligence, surveillance, and reconnaissance (C^4ISR)[4] systems. Although until recently commanders may not have thought of "achieving information superiority," all probably sought dominance in the information domain for the sake of facilitating "planning, directing, coordinating, and controlling [activities of] assigned forces"[5] to conduct operations without effective opposition.

With increasing reliance on C^4ISR systems, commanders protected their own systems by using, for example, cryptographic devices. They began to attempt to interfere with an adversary's electronic information system in order to deny that opponent the ability to plan, direct, coordinate, and so on, all in an effort to obtain the dominance in the information domain now called information superiority. In *Command in War*, Martin van Creveld described these developments as "an endless quest for certainty…a race between the demand for information and the ability of command systems to meet it."[6]

This report is about information superiority and the rationale for the development of a common direction for the modernization of C^4ISR systems. The report looks at Department of Defense (DOD) theory, employment, and modernization policies regarding C^4ISR systems in

---

[1]Martin van Creveld, *Command in War* (Cambridge, Mass.: Harvard University Press, 1985), 18.

[2]*Air Force Doctrine* (Washington, D.C.: The Pentagon, Air Force Doctrine Document 1, September 1997), 31.

[3]Martin van Creveld, *Technology and War* (New York: The Free Press, 1989), 235-236.

[4]The term C^4ISR systems evolved from command and control (C^2) systems and command, control, and communications (C^3) systems and is used to recognize the contributions of computer systems and intelligence, surveillance, and reconnaissance systems.

[5]See Frank M. Snyder, *Command and Control: The Literature and Commentaries* (Washington, D.C.: National Defense University [NDU] Press, Institute for National Strategic Studies [INSS], 1993), 11-12.

[6]*Command in War*, 264-265.

relation to their role in the newest warfare concepts, assesses aspects of employment and modernization of C^4ISR systems, and relates these systems to the overall goal of achieving information superiority.

The report has three goals: first—as the definitions given here suggest is needed—to clarify what the term information superiority means and how information superiority can be achieved; second, to ascertain whether information superiority can be measured by assessing the performance of C^4ISR systems during military operations; and, third, to explore two scenarios for improving the DOD's approach to modernization of C^4ISR systems and enhancing interoperability.

1.1 Ambiguity

The definition of information superiority according to the *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, was until very recently—January 1999—"that degree of dominance in the information domain which permits the conduct of operations without effective opposition."[7] This definition, as will be shown here, was challenged by other definitions of information superiority. The *Dictionary of Military and Associated Terms* now defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[8]

Although the term is vague, and vagueness gives reason for concern, its wide use has had some positive implications. However unclear, it has stimulated thought about information technology and the future of warfare. After all, in 1997–98 top Pentagon officials concluded that the United States must achieve information superiority. In early 1998, in a slide presentation, Arthur Money, the Chief Information Officer of the DOD, indicated that the "leadership's attention on C^3I/information superiority has dramatically increased" and that "information superiority is of critical and growing importance to military success."[9] Some consider it "the cognitive high ground in future conflict"[10]; others that it "will enable [U.S.] forces to know where

---

[7]*Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: The Pentagon, March 23, 1994), [On-line]. URL: <http://www.dtic.mil/doctrine/jel/doddict/> (Accessed Jan. 15, 1999.)

[8]Ibid. The new definition was approved, on Oct. 9, 1998, with approval of *Joint Doctrine for Information Operations*, Joint Publication 3-13 (Washington, D.C.: The Pentagon, Oct. 9, 1998), GL-7.

[9]Charts from slide presentation by Arthur L. Money, "C^3I, C^4ISR, Information Superiority," Washington, D.C., The Pentagon, May 11, 1998, slides 4 and 18.

[10]C. Edward Peartree, C. Kenneth Allard, and Carl O'Berry, "Information Superiority," in *Air and Space Power in the New Millennium*, edited by Daniel Goure and Christopher M. Szara (Washington, D.C.: Center for Strategic and International Studies, 1997), 128.

they are and where the opponent is."[11] Vision statements throughout the DOD prominently display information superiority as a goal to be achieved. In 1997, the U.S. Air Force, for example, declared information superiority a core competency,[12] and study groups have provided rationale supporting the need to achieve it. One study (completed in 1996) that concluded that the United States "must be able to achieve information superiority to assure victory in the future battlespace"[13] recommended making "an integrated C^4ISR system the highest investment priority of research, development, and procurement—equal in status to deployment of improved weapons systems."[14] The Defense Science Board 1998 Summer Study task force embraced information superiority and, at least loosely, began to establish a logical link to information operations.[15] The task force noted that superior capabilities "will be challenged by increasing international availability of state-of-the-art commercial products and services, particularly in the area of information superiority."[16]

Contributing to a common understanding of information superiority is important to this report, but a further aim is to suggest the implications of an evolving information domain for the conduct of military operations in the information age. The report accepts and builds on the definition of information superiority in the *Department of Defense Dictionary of Military and Associated Terms*, already cited, and proposes that the relationships between information operations and achieving information superiority are similar to those between air operations or maritime operations and achieving air or maritime superiority. For example, a declared goal of achieving air superiority is usually accomplished by conducting air operations primarily using air assets,[17] and, similarly, a declared goal of achieving maritime superiority is usually accomplished by conducting maritime operations using maritime assets.[18] When the goal of achieving information superiority is declared, it would be accomplished primarily by conducting

---

[11]Office of the Director for C^4 Systems, Joint Chiefs of Staff, *C^4I for the Warrior: A 1995 Progress Report* (Washington, D.C.: Pentagon [early 1996]), 4.

[12]Department of the Air Force, *Air Force Issues Book 1997*, Air Force Core Competencies, [On-line]. URL: <http://www.af.mil/lib/afissues/1997/issues23.html> (Accessed May 26, 1998.)

[13]Lawrence E. Casper, Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Steffens, and T. Lamar Willis, "Knowledge-Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly*, 13 (Autumn 1996), 88.

[14]Ibid.

[15]Department of Defense, Defense Science Board 1998 Summer Study Task Force, vol. 1, *Joint Operations Superiority in the 21st Century* (Washington, D.C.: The Pentagon, October 1998), 52.

[16]Ibid., 11.

[17]Will M. Jenkins, Jr., *The DOD's Changing Roles and Missions: Implications for Command and Control* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-96-5, May 1996), 57. Jenkins implied that in the Persian Gulf air supremacy was achieved through the actions of planners: "Air planners seized air superiority rapidly and paralyzed the Iraqi leadership's command structure with simultaneous air strikes against vital centers of gravity" (58).

[18]Ibid. According to Jenkins, writing on the Persian Gulf war, "Maritime operations provided naval supremacy for the impressive air campaign that followed" (57).

information operations using C^4ISR systems, that is, through these C^4ISR systems warriors would be provided with timely, reliable, and relevant information to the right place, allowing them to seize opportunities and accomplish objectives across the full range of military operations.[19] Hence, as air and maritime assets are the primary *capability* used to establish air and maritime superiority, the global grid of the C^4ISR systems is the *capability* that enables the establishment of information superiority over an adversary.

It has become fashionable to talk about achieving "information superiority" in the context of such new warfare concepts as network-centric warfare,[20] knowledge-based warfare,[21] C^2 warfare,[22] information warfare,[23] to name some of the trendiest. These concepts, and their underpinnings, derive from the information age and subscribe, in one form or another, to the notion of achieving information superiority. They do so even though what information superiority means often is unclear and even though the phrase has been used to describe a wide variety of circumstances. A spectrum of experts invoke information superiority as frequently as government leaders do patriotism or the clergy do sin.

This report proposes that information superiority can be regarded as air and maritime superiority are regarded, both of which are *conditions* that, at the start of a campaign, strategists and commanders attempt to achieve (and afterward to maintain) before other operations commence and use as a basis for those operations.[24] This report therefore suggests information superiority may be considered the same: *a condition achieved by means of information operations enabled by a global grid of C^4ISR systems* (see **Chapter Three**). And the report is offered in the hope that future military planners may come to think of information superiority in this way. As Michael P. Finn,[25] former Commander of the Naval Computer and Telecommunications

---

[19]*Doctrine for Command, Control, Communications, and Computer (C^4) Systems Support to Joint Operations*, Joint Publication 6-0 (Washington, D.C.: Pentagon, May 30, 1995) I-1.

[20]For an explanation of network-centric warfare, see Arthur K. Cebrowski, "Sea Change," *Surface Warfare* **22**, 6 (November–December 1997), 2-6. See also an interview with Cebrowski. "Network-Centric Warrior," *Military Information Technology* **2**, 2 (April–May 1998), 16-18.

[21]For an explanation of knowledge-based warfare, see Casper, et al., "Knowledge-Based Warfare: A Security Strategy for the Next Century," 81-89.

[22]For an explanation of C^2 warfare, see *Joint Doctrine for Command and Control Warfare*, Joint Publication 3-13.1 (Washington, D.C.: The Pentagon, Feb. 7, 1996.)

[23]For an explanation of information warfare, see Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: NDU Press, INSS, 1995.)

[24]Using the crisis and conflict in the Persian Gulf in 1990–91 as an example, *Joint Warfare of the Armed Forces of the United States*, Joint Publication 1, explains that gaining air superiority and maritime superiority were preconditions for further operations. It follows that air superiority and maritime superiority are to be considered conditions and therefore information superiority should be considered a condition. See *Joint Warfare of the Armed Forces of the United States*, Joint Publication 1, 2nd ed. (Washington, D.C.: The Pentagon, Jan.10, 1995), Appendix A, A-3, [On-line]. URL: <http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf> (Accessed March 12, 1998.)

[25]Personal communication by Michael P. Finn to Anthony G. Oettinger, Chairman of the Program on Information

Command, has pointed out, “information and information technology are among the major fueling agents of the revolutions in doctrine.”

1.2 The Role of Information Superiority in *Joint Vision 2010*

General Shalikashvili, the former Chairman of the Joint Chiefs of Staff, made information superiority central to his *Joint Vision 2010*[26] and created support for establishing and maintaining a capability for achieving it. He described information superiority as “the *capability* [emphasis added] to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.”[27] In mid-1997, in the Quadrennial Defense Review,[28] Secretary of Defense William Cohen supported information superiority as “the *ability* [emphasis added] to collect and distribute to U. S. forces throughout the battlefield an uninterrupted flow of information, while denying the enemy’s ability to do the same.”[29] Achieving information superiority is surely a necessary ingredient to assuring success in future military operations, but this report attempts to show that widely accepted descriptions of “information superiority” sidestep important issues. These descriptions hinder the scrutiny that “information superiority” needs and would otherwise receive were the term placed within a meaningful context and shown to be a condition similar to the conditions of air and maritime superiority.

Viewing information superiority as a condition, rather than as either a capability (General Shalikashvili) or ability (Secretary Cohen), could enhance debate by contributing to the formulation of answers to such questions as the following: (1) Is information superiority the desired outcome of successful information operations? (2) If so, what guiding principles are necessary to achieve information superiority? (3) What joint tactics, techniques, and procedures are necessary to implement these principles to achieve information superiority? And (4) what is the best modernization approach to lead to protected, integrated, and interoperable C^4ISR systems capable of achieving information superiority?

Until such questions, and others, are addressed, information superiority will continue to be something everybody wants but with no clear sense of direction toward what to do to achieve it.

Resources Policy, Harvard University, Nov. 25, 1998.

[26]Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: The Pentagon [1996]), 16. Hereafter cited as *Joint Vision 2010*.

[27]Ibid., 16.

[28]The Quadrennial Defense Review (QDR), completed in May 1997, was a comprehensive analysis of the DOD’s strategies, force structure, and modernization programs for the period 1997–2015. The final report based on the QDR is available [On-line] at URL: <http://www.defenselink.mil/pubs/qdr> (Accessed March 9, 1998.)

[29]William S. Cohen, Secretary of Defense, in “The Secretary’s Message,” in “What’s New?” *Report of the Quadrennial Defense Review* (Washington, D.C.: The Pentagon, May 1997) [On-line]. URL: <http://www.defenselink.mil/pubs/qdr/msg.html> (Accessed March 10, 1998.)

Information superiority, this report suggests, should be considered a condition to be achieved through effective information operations while using protected, integrated, and interoperable C^4ISR systems as the capability.

1.3 Think Joint!

General Shalikashvili's *Joint Vision 2010* put a mark on the wall for achieving "higher levels of jointness,"[30] that is, optimizing the mix of ground, maritime, and air forces so they can achieve "synergism" during military operations.

Synergism, as a term applied to the conduct of military operations, was first used by Admiral William A. Owens, former Vice-Chairman of the Joint Chiefs of Staff.[31] Synergism, it is postulated here, may be made possible by new operational concepts, the acceptance of maturing joint doctrine by military leaders, who, in increasing numbers, are participating in joint military education and—since the 1986 Goldwater–Nichols Reorganization Act[32]—serving in joint assignments, as well as the ever increasing application of supporting joint tactics, techniques, and procedures in military operations.

To synchronize combat and create the simultaneous massed effects envisioned in *Joint Vision 2010* (see **Figure 2-1**), the DOD will need to ensure that any joint force engaged in military operations can share information. It sounds elementary, but engaging in synchronized military operations increases the importance of protected, integrated, and interoperable future C^4ISR systems. The alternative would be a continuation of incremental improvements on old concepts "that were largely sequential in nature…[and] saw ground, maritime, and air forces massed in time and space."[33]

1.4 Experimentation

Publication of *Joint Vision 2010* sparked questions on how to achieve information superiority as well as answers that, as this report shows, are neither simple nor near being put to rest. For the moment (1999), experimentation has emerged as both the key strategic element in the DOD's quest for information superiority[34] and as a way to keep abreast of information-age

---

[30]Gen. John M. Shalikashvili, "A Word from the Chairman," *Joint Force Quarterly*, 12 (Summer 1996), 5.

[31]Adm. Owens used "synergism" to mean that "higher combat effectiveness is made possible by combining forces in such a way that higher outputs result than could be achieved by simply adding the outputs of different forces" (Owens, "Living Jointness," *Joint Force Quarterly*, 3 [Winter 1993–94], 7).

[32]Goldwater–Nichols Department of Defense Reorganization Act of 1986, Public Law 99-433, Oct.1, 1986.

[33]*Joint Vision 2010*, 17.

[34]According to Lt. Gen. Douglas Buchholz, "Experimentation is emerging as a key element of [the DOD's] strategy for implementing information superiority." See Buchholz, "Joint Dominance; Paving the Way for Information Superiority in the 21st Century," *Military Information Technology* **1**, 3 (October–November 1997), 20.

innovations. General Henry H. Shelton, Chairman of the Joint Chiefs of Staff (CJCS) since October 1997, called for "information superiority experiments to test concepts and capabilities vis-à-vis the information revolution."[35] He added that "joint experimentation" can be a means to assess *Joint Vision 2010* concepts and develop new capabilities.[36] Senator Dan Coats (Rep.-Ind.), chairman of the Senate Armed Services Committee (SASC), 105th Congress (1997–98), supports General Shelton's view on experimentation. According to Coats, "a joint experimentation process can serve as the basis for investment decisions both in the Pentagon and on Capitol Hill."[37] He recognized that "the services jealously guard dwindling force structures, systems, and platforms."[38]

General Shelton also identified another major challenge associated with *Joint Vision 2010* experimentation: "where will the dollars, people, equipment, and time for joint experimentation come from?"[39] A strategy of joint experimentation can undoubtedly yield immediate improvements, but, as an indirect challenge to the traditional modernization process, it could also raise further questions concerning how results of experimentation might be implemented.

If the Chairman's push for information superiority experiments (ISXs)[40] were to lead to resources being made available to conduct them, C^4ISR systems capabilities could emerge. In that circumstance, the DOD would face a situation not entirely new—that is, a whole host of questions for answers needs to be found. Some questions are new. How do C^4ISR systems capabilities that have been proved successful in a joint experiment (as opposed to capabilities proved successful in a service experiment) find their way into the hands of the joint warriors that need them? Who will procure these capabilities, and when? How will these new capabilities stack up against capabilities desired by a service? Will they undergo systems interoperability certification testing? How will operations and maintenance costs be dealt with, and how will the training base accommodate the new systems? As yet, no effective mechanism for fielding protected, integrated, and interoperable C^4ISR systems stemming from similar experiments—

---

[35]Gen. Henry H. Shelton, "A Word from the New Chairman," *Joint Force Quarterly*, 17 (Autumn–Winter 1997-98), 6.

[36]Ibid., 7.

[37]Dan Coats, "Joint Experimentation—Unlocking the Promise of the Future," *Joint Force Quarterly*, 17 (Autumn–Winter 1997–98), 18.

[38]Ibid., 19.

[39]Shelton, 8.

[40]Although, as of the writing of this report, the DOD has not published a formal explanation for the Information Superiority Experiments (ISXs), the term appears prominently in "The Emerging Joint Strategy for Information Superiority," a Joint Staff slide presentation; see slides 57–60. [On-line]. URL: <http://www.dtic.mil/jcs/j6/edu_tr.html> (Accessed April 17, 1998.)

such as Advanced Concepts Technology Demonstrations (ACTDs)[41] and Joint Warrior Interoperability Demonstrations (JWIDs)[42]—has been devised.

As this report shows, conducting C4ISR experiments, even joint C4ISR experiments, is not new, and some issues related to such experiments have already been seen to require resolution. If the DOD's aim is to conduct joint experiments that will yield protected, integrated, and interoperable C4ISR systems capable of achieving information superiority, then a comprehensive process to address the questions posed in the previous paragraph, among others, needs to be formulated, documented, and institutionalized.[43]

1.5 Organization of the Discussion

The discussion here is based on five premises: (1) that the DOD is committed to achieving information superiority[44]; (2) that the C4ISR portion of the overall DOD budget will not be increased[45]; (3) that, for reasons of effectiveness and efficiency, joint and combined operations are

---

[41]The Advanced Concepts Technology Demonstration process is a preacquisition stage process that provides a mechanism for the warfighter to evaluate proposed solutions to urgent military needs. An ACTD provides a warfighter with a prototype capability and allows the use of that capability in realistic operational scenarios, thus allowing the warfighter to refine operational requirements, develop a concept of operations, and make determinations of the military utility of a proposed solution prior to entering the formal acquisition process. The ACTD process evolved in 1994 in response to recommendations of the Packard Commission (1986) and the Defense Science Board (1987, 1990, 1991).

[42]JWIDs, sponsored by the Joint Staff, are annual demonstrations of evolving low-cost, low-risk C4I technologies and joint interoperability solutions, presented impartially to the CINCs and Military services in an operational environment. Specific demonstrations fulfill identified warfighter deficiencies and are designed to provide an opportunity to experiment with evolving capabilities, assess their value, and recommend them for implementation where appropriate.

[43]Some issues that need resolution as part of such a comprehensive mechanism have emerged in 1998 and others have been around for a while. One issue recently surfaced in the General Accounting Office (GAO)/National Security and International Affairs Division (NSIAD) Report, *Joint Military Operations; Weaknesses in DOD's Process for Certifying C4I Systems' Interoperability* ([Washington, D.C.: GAO/NSIAD 98-73, March 1998], 5), according to which "during the last three years, no systems purchased through the ACTD program were tested and certified" for interoperability. Another example is that funding for fielding systems successfully demonstrated in JWIDs has to date not been available. The Joint Chiefs of Staff Instruction 6260.01, *Joint Warrior Interoperability Demonstrations* (Washington, D.C.: The Pentagon, Sept. 15, 1998) attempts to find a solution to this problem. It promulgates the necessary policy to conduct JWIDs on a two-year cycle rather than an annual one. The policy describes one year as a "theme" year, when C4I demonstrations will be conducted, followed by an "exploitation year," when JWID "Golden Nuggets" will be acquired and distributed. Adoption of the two-year cycle is intended to facilitate fielding C4I solutions without increasing overall JWID outlays.

[44]William S. Cohen, Secretary of Defense, "Transforming U.S. Forces for the Future" Section VII, *Report of the Quadrennial Defense Review* (Washington, D.C.: The Pentagon, May 1997) [On-line]. URL: <http://www.defenselink.mil/pubs/qdr/sec7.html> (Accessed March 9, 1998.)

[45]Ibid. In "What's Next—How Do We Get From Here to There?" "The Secretary's Message," Cohen concluded that the "amount of resources devoted to this effort were determined to be appropriate." See [On-line]. URL: <http://www.defenselink.mil/pubs/qdr/msg.html> (Accessed Oct. 12, 1997.)

embedded in the backbone of the U.S. military[46]; (4) that the DOD desires to conduct future military operations by taking advantage of the synergism—to use Admiral William Owens's word[47]—made possible by optimizing and blending the capabilities of each force component (ground, maritime, and air), thereby developing and using a multidimensional capability more powerful than any past joint force; and (5) that for a joint force to conduct synchronized military operations depends on the DOD's ability to employ and modernize protected, integrated, and interoperable C^4ISR systems.

The value of C^4ISR systems, whose development, as already indicated, has been heavily debated over many years, and of information exchange, particularly among battle-management centers, sensors, combat-direction platforms, weapons platforms, and among weapons themselves, during synchronized military operations, is the subject of **Chapter Two**, with a particular focus on the capability—the C^4ISR systems themselves—required to achieve information superiority.

Chapter Three traces information superiority to its origins in the DOD and presents various interpretations of the term. It introduces the *C^4I for the Warrior*[48](C^4IFTW) vision and shows how both the term and the ideas embodied in it have evolved. It concludes by offering a different view of what information superiority may consist of and mean.

Chapter Four is devoted to the development of a useful six-point scale (similar to the Defense Readiness Conditions),[49] to identify information domain conditions—information inferiority, disadvantage, parity, advantage, superiority or supremacy—that obtain during a military operation. It attempts to move information superiority from the theoretical realm into the practical.

Chapter Five attempts to answer the question of whether an information domain condition, that is, information superiority, can be measured by assessing the performance of C^4ISR systems in past military operations. Two military operations now judged successful are examined in this

---

[46]*Joint Warfare of the Armed Forces of the United States*, Joint Publication 1, 2nd ed.

[47]See Jeffrey R. Cooper, "Dominant Battlespace Awareness and Future Warfare," in *Dominant Battlespace Knowledge* edited by Stuart E. Johnson and Martin C. Libicki (Washington, D.C.: NDU Press, INSS, 1995), 112; and Williams Owens in "Living Jointness," *Joint Forces Quarterly*, 3 (Winter 1993–94), 7-14. Admiral Owens was Vice Chairman of the Joint Chiefs of Staff, 1994–96, and in 1998 he became vice chairman and chief executive officer of the Teledesic Corp.

[48]Office of the Director for C^4 Systems, The Joint Staff, *C^4I for the Warrior* (Washington, D.C.: The Pentagon, June 12, 1992).

[49]According to the *Department of Defense Dictionary of Military and Associated Terms*, previously cited, Defense Readiness Conditions (DEFCON) are "A uniform system of progressive alert postures for use between the Chairman of the Joint Chiefs of Staff and the commanders of unified commands and for use by the services. Defense readiness conditions are graduated to match situations of varying military severity (status of alert). Defense readiness conditions are identified by the short title DEFCON (5), (4), (3), (2), and (1), as appropriate."

light, the invasion of Grenada in 1983[50] and the Persian Gulf war in 1990–91,[51] an international effort undertaken by a coalition forged for the particular occasion.

Chapter Six looks at the current and future C^4ISR capability, which is expected to achieve information superiority. Two scenarios are explored in an effort to identify opportunities to improve the DOD's C^4ISR approach to modernization and its enhancement of interoperability in support of future warfare concepts.

Chapter Seven summarizes the main points of the report.

Despite an effort to keep the report as free as possible of acronyms and jargon, their use has been at times unavoidable. The hope is that when jargon is used here it is adequately explained. All acronyms used in the text appear in the list at the end of this report. Given the subject matter, certain of them are inevitable and appear frequently: command and control (C^2) systems, command, control, and communications (C^3) systems, command, control, communications, and computer (C^4) systems, and command, control, communications, computer, and intelligence (C^4I) systems. These terms have evolved over time, and in recent years C^4ISR systems has become the one favored in the Pentagon, invoked, for example, when the DOD (with considerable effort) developed a C^4ISR Architecture Framework,[52] conducted a C^4ISR Mission Analysis (CMA),[53] and established a Joint C^4ISR Battle Center[54] and C^4ISR Decision Support Center.[55] In line with these

---

[50]For a complete discussion of the invasion of Grenada, beginning with the contingency planning for noncombatant evacuation after the coup on Oct. 12, 1983, which removed Grenada's Marxist leader, Maurice Bishop, and ending with the combat phase of operation Urgent Fury on Nov. 2, 1983, see Ronald H. Cole, *Operation Urgent Fury: Grenada* (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, Joint History Office, 1997).

[51]For a complete discussion of the Persian Gulf war, see the U.S. Department of Defense, *Conduct of the Persian Gulf War*, Department of Defense Final Report to Congress (Washington, D.C.: The Pentagon, April 1992).

[52]Department of Defense, C^4ISR Architecture Working Group, *C^4ISR Architecture Framework* (Washington, D.C.: The Pentagon, Dec. 18, 1997), [On-line]. URL: <http://www.cisa.osd.mil/hostedsites/index.htm> (Accessed Feb. 10, 1998.)

[53]The CMA was an analytical effort undertaken by the Office of the Assistant Secretary of Defense for C^3I and the Joint Staff (J6) from July '96 to February '97 in response to FY98-03 Defense Planning Guidance and recommendations from several Defense Science Board studies and Commission on Roles and Missions findings. The goals of the CMA were to develop a C^4ISR investment strategy to guide future program and budget development and to produce C^4ISR architecture frameworks to guide the integration of C^4ISR systems.

[54]The Joint C^4ISR Battle Center, in Suffolk, Va., was established in 1996 to provide an experimental environment to facilitate rapid, near-term insertion of C^4ISR technology. See Office of the Chairman of the Joint Chiefs of Staff Memorandum, Subject: "Revised Charter of the Joint C^4ISR Battle Center" (Aug. 20, 1997), [On-line]. URL: <http://www.jbc.js.mil/public/docs/papers/charter.pdf> (Accessed March 6, 1998.)

[55]The Joint C^4ISR Decision Support Center, in Crystal City, Va., was established in 1996 to conduct quantitative and qualitative analysis to support C^4ISR requirements and acquisition decisionmakers. See Office of the Assistant Secretary of Defense for C^3I Memorandum, Subject: "Joint C^4ISR Decision Support Center Implementation Plan" (Jan. 27, 1997), [On-line]. URL: <http://www.cisa.osd.mil/organization/dsc/ImpPlan/ipapprv.pdf> (Accessed March 6, 1998.)

and other integration efforts and to acknowledge this evolution, this report uses the acronym C^4ISR throughout.

Chapter Two

C^4ISR and Its Pivotal Role in the Information Age

This chapter introduces the notion that in 1999 information operations can be considered as much a core dimension in the overall planning for future military operations as maritime and air operations were in earlier years. The focus is on the capability—the C^4ISR systems themselves—required to achieve information superiority, and both the much debated development of these systems in the DOD and their role in information operations are discussed.

2.1 Warfare in the Information Age

The United States's military is the best in the world. It is the most capable, best equipped force on the planet, and potential adversaries know that. Although the likelihood that an adversary will engage the U. S. head-on is slim, the possibility cannot be ignored. But in addition to such direct threats, the U.S. has to consider the possibility of a relatively new and serious growing threat: unauthorized access to computer based systems. In 1998, in a televised interview, Secretary of Defense Cohen discussed the possibility of potential adversaries launching attacks on this Achilles' heel. Such an attack, he said, could "come in the form of cyber-terrorism, whereby you have hackers[1] who will back into our critical infrastructure seeking to bring down either our banking system, Wall Street, our transportation systems [or] energy systems."[2] Although the Secretary did not specifically mention the DOD's vulnerabilities to cyber-attacks from unknown and unauthorized individuals, such vulnerabilities exist and computer attacks against the DOD pose increasing risks.[3]

---

[1]According to the GAO report *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* ([Washington, D.C.: GAO, GAO/Accounting and Information Management Division (AIMD)-96-84, May 1996], 2), the term "hackers" has a relatively long history. At one time, it signified persons who explored the inner workings of computer systems to expand their capabilities, as opposed to those who simply used computer systems; in 1998, the term is generally used to mean unauthorized persons who attempt to penetrate information systems to browse, steal, or modify data, or to deny access or service to others, or in some other way to cause damage or harm.

[2]In 1998, William S. Cohen, Secretary of Defense, speaking of the U. S. military, said that "we are the best in the world and the strongest in the world, the most capable, the most highly educated, the best led, best equipped force in the world today—by virtue of that strength, very few countries will seek to take us on head-on." Televised interview with Cohen by Charlie Rose on "Crosstalk," "Preparing the Military for the 21st Century," Washington, D.C., Jan. 6, 1998. For information on a national strategy to protect critical infrastructures from cyber threats, see the Final Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure* (Washington, D.C.: The White House, October 1997), [On-line]. URL: <http://www.pccip.gov/report_index.html> (Accessed July 20, 1998.)

[3]For a report on such vulnerabilities see *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. For a technical primer on cyber risks, see Executive Office of the President of the United States, *Cybernation: The American Infrastructure in the Information Age* (Washington, D.C.: The White House, April 1997).

"Crucial to information superiority," claimed the Joint Staff in 1998, "is the emerging concept of network-centric warfare."[4] But have not information and the ability to collect, process, and disseminate it always been central to warfare? In the information age, will U. S. forces really conduct network-centric warfare, or will they still conduct plain old warfare? Networks will of course be essential to military operations in the information age. The availability in all future military operations of a network of C^4ISR systems to facilitate the exchange of information among battle-management centers, sensors, combat-direction platforms, weapons platforms, and among the weapons themselves may be assumed to be critical, but will that be so whether warfare is called network centric, knowledge based, or just plain warfare?

2.1.1 Network-Centric Warfare

The Defense Science Board 1998 Summer Study task force concluded that a new strategy was needed for an integrated target engagement capability. Such a strategy, the task force offered, needed to exploit the "new generation of integrated sensor capabilities, distributive interactive C2, targeting based on desired effects [etc.]…and a ubiquitous integrated system infrastructure."[5] The task force essentially recommended expansion of what in 1999 is known as network operations.[6]

In 1998, in an interview published in *Military Information Technology,* Vice Admiral Arthur K. Cebrowski, at that time the Navy's Director for Information and Electronic Warfare, described network-centric warfare as

> the application of combat power from widely dispersed but very robustly netted forces to alter initial conditions, develop very high rates of change, and achieve the desired outcome of locking in success and locking out alternative enemy strategies.[7]

This description, although framed specifically to describe network-centric warfare, may be appropriate also to describe the conduct of a variety of military operations in the information age, and as a visionary concept it may be applied generally to future warfare. Maximizing the value of the network, which is Cebrowski's premise, highlights the importance of interfaces and interconnections and would support the view held in this report that protected, integrated, and

---

[4]Office of the Director for C^4 Systems, The Joint Staff, *C^4I for the Warrior: The Joint Vision for C^4I Interoperability* (Washington, D.C.: The Pentagon, January 1998), 20.

[5]Department of Defense, Defense Science Board 1998 Summer Study Task Force, vol. 1, *Joint Operations Superiority in the 21st Century* (Washington, D.C.: The Pentagon, October 1998), 63.

[6]Network operations comprise three elements: information dissemination management; network management; and information assurance.

[7]Interview with Vice Adm. Arthur K. Cebrowski, "Network-Centric Warrior," *Military Information Technology* **2**, 2 (April–May 1998), 16.

interoperable C4ISR systems will be pivotal to enabling future joint warriors to achieve information superiority.

But in the view of Walter Jajko, Professor of National Security Studies at the Institute of World Politics, achieving information superiority is only the means to an end—it allows one "to apply decisive force, to break the enemy physically or psychologically" and "its ultimate aim is victory for a political objective."[8]

Future C4ISR systems, which are expected to support synchronized military operations, will probably support widely dispersed joint forces operating under pressure of time for which they will need to be designed. This report suggests that if this projected future is what lies behind the many uses of the term "information superiority," then the opportunities of actually fielding such systems might be considerably enhanced by a transformation of the overall process of modernization of C4ISR systems. To accomplish this transformation, the current (1999) modernization process would need to change so that requirements would be developed to support a joint military force, systems designs would be optimized for synchronized operations, and C4ISR systems would be engineered as part of a network that would ultimately be capable of achieving information superiority over an adversary. Thus, these endeavors would seem to be dovetailed and inseparable.

2.1.2 Breaking Familiar Practices

In 1997, in *Surface Warfare*, Admiral Cebrowski explained today's reliance on network information as a shift from platforms to networks:

> Just a few years ago, the stand-alone computer or workstation was the high-end of computer use, and computer users sought to have the greatest possible capability in their platform. Today, the focus of information systems has shifted away from this "platform-centric computing" to "network-centric computing," in which the greatest possible capability is resident in the network to which the workstation is connected. The network provides vastly increased capability to the end users by increasing the amount of information available to them, accelerating the rate of information transfer and decreasing decision delay.[9]

If Admiral Cebrowski and others[10] are correct in recognizing the transition of the military from platform-centric computing to network-centric computing in support of future military operations

---

[8]Personal communication (more extensive than could be included in entirety) by Walter Jajko, Brigadier General, USAF (Ret.), to Anthony G. Oettinger, Nov. 10, 1998.

[9]Arthur K. Cebrowski, "Sea Change," *Surface Warfare* **22**, 6 (November–December 1997), 5.

[10]See Clarence A. Robinson, Jr., "Warfighter Information Network Harnesses Simulation Validation," *Signal Magazine* **52**, 5 (January 1998), 27.

that are synchronized, then planning for modernization of integrated C^4ISR systems optimized to support a joint force will be more important than ever before.

Such planning will also be infinitely more complex than current Pentagon processes can accommodate. Traditional barriers between the services may need to be broken and policies revised. For example, loopholes that now (1999) permit the services to develop C^4 capabilities independently, with limited regard for integrating the needs of other services, may need to be eliminated. The C^4 and ISR communities will both need to find ways, where practical, to integrate requirements and field integrated system capabilities. And computer resources that are part of weapons systems may need to be linked to the overall C^4ISR network, requiring the development of new software policy, an area for which responsibility and oversight appear unnecessarily confusing.[11]

2.1.3 Optimizing the Flow of Information

Improving the flow of information among battle-management centers, sensors, combat-direction platforms, weapons platforms, and among computer resources which are themselves part of weapon systems offers enormous potential for facilitating the accuracy and lethality of modern combat weapons. This potential was recognized by Admiral William Owens, USN, Ret., and was a theme of his efforts during his tenure as Vice Chairman of the Joint Chiefs of Staff (VCJCS) to influence the services to consider the interrelationships between C^4ISR systems and weapons systems.[12] As part of these efforts, Admiral Owens wrote and spoke regularly on the potential benefits of a synergy derived from these relationships. He consistently focussed on outdated DOD practices and urged military and civilian leaders to insist on the revamping of the DOD's planning and programming processes.

> Something about the way we plan and program in the Defense Department keeps us in compartmented perspectives. We are more adept at seeing some of the individual trees than that vast forest of military capability the

[11]Department of Defense, *Assistant Secretary of Defense for Command, Control, Communications, and Intelligence*, Directive 5137.1 ([Washington, D.C., The Pentagon, Feb. 12, 1992], 2), exempts the ASD(C^3I) from the responsibility for establishing software policy and practices related to computer resources, both hardware and software, that are "physically part of, dedicated to, or essential in real time to the mission performance of weapon systems; used for weapon system specialized training, simulation, diagnostic test and maintenance, or calibration; or used for research and development of weapon systems."

[12]For a discussion of the interrelationships between information technology and weapons systems, see William A. Owens, "The Three Revolutions in Military Affairs," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1995* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-96-2, January 1996), 29-48.

> individual systems are building, so it is easy to miss the fact that, together, these programs posit a qualitatively different military potential.[13]

As the DOD's dependence on network-based support systems increases with applications of new technologies, the views of Admirals Owens and Cebrowski deserve consideration.

The ability to achieve information superiority will be crucial not only to network-centric warfare support systems but also to other new force structure and warfare concepts in the foreseeable future. As already suggested (see section **1.3**), whether the DOD will be able to field protected, integrated, and interoperable C^4ISR systems will be critical to its ability to synchronize combat and create simultaneous massed effects such as envisioned in *Joint Vision 2010* (see **Figure 2-1**). Acceptance of Admiral Owens's and Cebrowski's argument offers a basis for framing the objectives as comprehensive military capabilities,[14] rather than treating advances in the weapons platforms and C^4ISR systems as discrete and separate as the application of new technologies increases the DOD's dependence on network based support systems.[15]

2.2 Other Factors and Consequences

The information age promises not only new efficiencies but also factors and consequences that the military has never before needed to contemplate, factors too numerous to enumerate, each of which could be the subject for another report, although a few too significant to ignore are mentioned here briefly.

Consider how information can itself be used as a weapon.[16] Not to give attention to this as an option would be to be naïve. Future efforts to modernize C^4ISR systems will need to include options such as this, which could provide commanders with offensive capabilities to achieve information superiority. For example, C^4ISR systems could include electronic intrusion capabilities, e.g., to launch a virus or a logic bomb against an adversary's C^2 systems. This option could provide operational commanders with effective information weapons to supplement traditional capabilities.[17]

Other considerations come along with information-age technology. Anyone with a telephone line and a terminal can introduce a glut of information into cyberspace, something that

---

[13]William A. Owens , "Introduction," *Dominant Battlespace Knowledge*, edited by Stuart E. Johnson and Martin C. Libicki (Washington, D.C.: NDU Press, 1995), 4.

[14]Such an overall military capability could include force structure, a supporting systems structure, and even a warfare strategy.

[15]Owens , "Introduction," *Dominant Battlespace Knowledge*, 4.

[16]For further detail, see Maj. YuLin Whitehead, "Information as a Weapon: Reality versus Promises," *Airpower Journal* **11**, 3 (Fall 1997), 41-53.

[17]Ibid., 52.

should both make military planners cautious and spur initiatives on ways to guard against information overload. Military planners will need to ensure that the information traversing the C^4ISR network remains relevant, protected, and reliable.

2.3 Money, Optimism, and a New Operational Framework

With Congress providing billions of dollars every year for C^4ISR programs, expectations for future C^4ISR systems are high. Achieving information superiority will be expensive. Forecasting the costs associated with this goal is difficult. No one really knows how much the DOD annually spends on information technology. Much of the money spent on DOD information technology programs is hidden in budget lines for a variety of reasons. Many estimate that roughly $50 billion dollars per year is spent for C^4ISR systems and activities. In 1998, the General Accounting Office (GAO)[18] reported that "based on its analysis of the fiscal year 1999 through 2003 Future Years Defense Plan, DOD estimates it will budget an average of $43billion a year for C4ISR systems and activities…."[19] According to an estimate by Duane Andrews, a former Assistant Secretary of Defense for C^3I, now executive vice-president for Science Applications International Corporation (SAIC), in 1998 "the direct C^4ISR and IT [information technology] expenditures of the Department of Defense total about $50 billion per year."[20] Similarly, in 1997, the Electronic Industries Association (EIA) claimed in a press release that "the Pentagon now spends over $50 billion per year to buy and operate information-related systems."[21] Although locating Congressional sources that corroborate this figure are not easy to find, a report of the Defense Subcommittee of the House Appropriations Committee for the 103rd Congress disclosed that the overall "request for C^3I programs totals $50.6 billion in fiscal year 1995."[22]

If these estimates are accurate, even with a new vision of information superiority, can additional money from the roughly $250 billion per year defense budget be expected to go to C^4ISR? Probably not. The resources needed to achieve information superiority are more likely to be found in elimination of obsolete and duplicative systems and in deliberate trimming of overall

---

[18]A nonpartisan agency within the legislative branch of the government, the GAO conducts audits, surveys, investigations, and evaluations of federal programs. Work is done at the request of congressional committees or members, or to fulfill requirements mandated by the GAO or the legislative branch. The GAO's findings and recommendations are published as reports to Congress or delivered as testimony to congressional committees.

[19]U.S. GAO/NSIAD, *Defense Information Superiority: Progress Made, but Significant Challenges Remain* (Washington, D.C.: GAO/NSIAD/AIMD-98-257, August 1998), 2.

[20]Duane Andrews, A Recommended Blueprint for the ASD(C^3I) and CIO in Response to DRI Directive #17 (McLean, Va.: SAIC, March 11, 1998), 13 (unpublished).

[21]Electronic Industries Association (EIA), "EIA Foresees Major Market and High Hurdles in Information Superiority," press release, Oct. 9, 1997, [On-line]. URL: <http://www.eia.org/pad/press/files/9710/97-62.htm> (Accessed April 1, 1998.)

[22]U.S. House of Representatives, Committee on Appropriations, Subcommittee on the Department of Defense, *Department of Defense Appropriations for 1995* (Washington, D.C.: U.S. Gov't Printing Office, 1994), Part 3, 777.

support costs. Further, new C^4ISR capabilities will need to be developed with an eye to integrating the requirements that lead toward a C^4ISR network that is protected, integrated, and interoperable and which would provide joint warriors with timely, reliable, and relevant information to allow joint forces to seize opportunities and meet objectives across a full range of military operations,[23] regardless of which service owns which system.

Expectations that demands for protected, integrated, and interoperable C^4ISR systems can be met are widely optimistic, on the basis of theory that U.S. companies can produce improved C^4ISR systems to "support more efficient information fusion and multimedia, multifunctional [processing]"[24] that will lead to making more timely, reliable, and relevant information available to decisionmakers while denying an adversary any operational advantage in the information domain. The promise of continual advancement in technologies and, most important, a focus on developing new operational capabilities[25] enabled by these systems served as the foundation of General Shalikashvili's new operational framework of dominant maneuver, precision engagement, focussed logistics, and full-dimensional protection (see **Figure 2-1**), outlined in *Joint Vision 2010*.

2.4 Cautions, Wisdom, and Criticism

Commanders need to be able to maintain control over widely dispersed forces, thereby enhancing agility and mobility while executing complex operations. C^4ISR systems could form the network that could provide commanders this ability, but as long as these systems remain service specific, the systems cannot do so. Given the technological advantage of the United States, with no challenger on the horizon, evolution toward a C^4ISR network capable of achieving information superiority over any adversary at any time is well within reach, but such an evolution from what is currently [1999] in place would require changes in the DOD's process of modernizing C^4ISR systems.

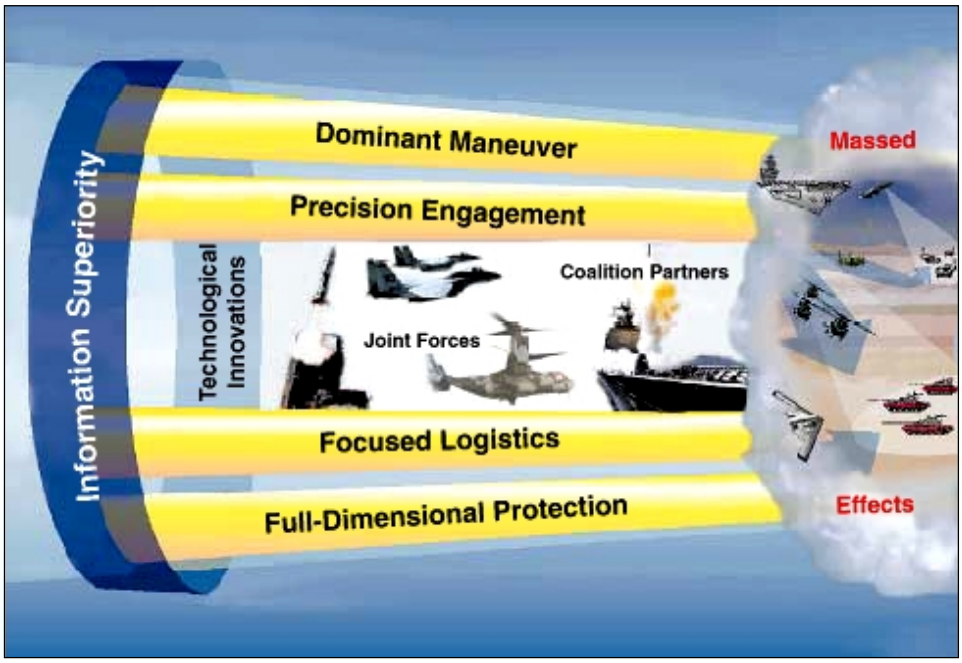
The DOD's information technology community will need to develop plans to move from current C^4ISR capabilities to an integrated C^4ISR network. If it does not do so, this community may stay on the receiving end of criticism not only from warriors within the military but also

---

[23]See *Doctrine for Command, Control, Communications, and Computer (C^4) Systems Support to Joint Operations*, Joint Publication 6-0 (Washington, D.C.: The Pentagon, May 30, 1995), I-1.

[24]The Joint Warfighting Center, *Concept for Future Joint Operations: Expanding Joint Vision 2010* (Ft. Monroe, Va.: Joint Warfighting Center, May 1997), 43.

[25]In "A Word from the Chairman" (*Joint Force Quarterly*, 12 [Summer 1996], 5), Gen. Shalikashvili stated that *Joint Vision 2010* is less about technology than the development of new operational capabilities.



Source: Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: The Pentagon [1996]), 19.

Figure 2-1

Emerging Operational Concepts

from members of Congress, the GAO, congressional staff such as the House Appropriations Committee (HAC) Survey and Investigations (S&I) teams, analysts, and journalists that cover the DOD. Examples of criticism are plentiful. Consider the special report in *Federal Computer Week Online*[26] by Bob Brewin, who, referring to the DOD's current C^4ISR capability, noted that "the Defense Department did not plan the current hodgepodge of networks that has grown up with the decade-long evolution of client/server computing,"[27] thus making clear he was unimpressed by the DOD's overall planning.

The DOD will also need to establish both parameters and criteria which its C^4ISR systems will have to meet before these can reasonably be expected to contribute to achieving information superiority. One example would be that a C^4ISR system must demonstrate that it will meet criteria for interoperability set forth in appropriate DOD regulations[28] and thus can be certified as

[26]Bob Brewin, "DOD Lays Groundwork for Network-Centric Warfare," *Federal Computer Week Online*, Editorial Supplement (Nov. 10, 1997), [On-line]. URL: <http://www.fcw.com/pubs/fcw/1997/1110/wp/fednets.htm> (Accessed March 7, 1998.)

[27]Ibid.

[28]The DOD's primary interoperability guidance documents are DOD Directive 4630.5, Nov. 12, 1992; DOD Instruction 4630.8, Nov.18, 1992; Chairman of the Joint Chiefs of Staff Instruction 6212.01A, June 30, 1995; and Defense Information Systems Agency, JIEO/JITC Circular 9002, Jan. 23, 1995.

interoperable. Without such criteria, and others like it, for example, information security criteria, the DOD cannot even know whether it is on the right path toward information superiority. To date, even though the DOD has not said how it plans to achieve information superiority, some, citing problems of interoperability and serious shortfalls in information security, have already opined that its efforts in this direction are far from adequate.[29]

Others point to problems in military culture as critical, among them Alan Campen, the manager of the Armed Forces Communications and Electronics Association (AFCEA) Press and adjunct professor at the School of Information Warfare and Strategy at the National Defense University. Campen has described today's military culture as favoring "military service requirements more than it does those of the joint forces commander."[30] This observation may strike a chord with those knowledgeable about past problems. If true, it suggests a military that would field C^4ISR systems less than optimal for executing joint operations. Campen's counsel ought not be ignored, especially as others writing on the DOD's C^4ISR systems support his views.

Author and C^2 scholar Kenneth Allard has offered counsel from a different perspective. In the revised edition (1996) of *Command, Control, and the Common Defense*, Allard examined problems that the DOD has had in the past in fielding integrated and interoperable C^2 systems. Without necessarily being critical of the DOD's approach, Allard made the point that "services organized and equipped on the basis of essential differences tend to do things the Army way, the Navy way, the Air Force way, and the Marine way."[31]

Allard's views are respected by many, including Senator Chuck Robb (Dem.-Va.), a member of the SASC, who paraphrased Allard during a Senate hearing in 1998 when he posed the following question to a group of defense experts serving on the National Defense Panel[32]:

> if American military forces are on the same side, then why do [they] still have a problem talking to each other? And when the Internet links millions of disparate users, why do our forces still develop and procure separate command and control information systems, [in] which duplication is a constant and interoperability, an afterthought.[33]

---

[29]According to Andrews, in *A Recommended Blueprint for the ASD(C^3I) and CIO…* (7), "Today, the Department's information systems and activities would not meet any reasonable test of information superiority."

[30]Alan D. Campen, "Joint Vision Initiates Big Challenge to Acquisition, Integration, Culture," *Signal Magazine* **52**, 2 (October 1997), 71.

[31]Kenneth Allard, *Command, Control, and the Common Defense*, rev. ed. (Washington, D.C.: NDU Press, October 1996), 18.

[32]The National Defense Panel was asked to provide Congress and the Secretary of Defense with an independent review of national security requirements, including the force structure necessary to meet them. The nine-month task, completed in January 1998, provided alternatives to the recommendations in the QDR.

[33]U.S. Senate, Committee on Armed Services, *Hearings on the National Defense Panel* (Washington, D.C.: Federal Information Systems Corporation, Federal News Service, Jan. 28, 1998), [n. p.].

The experts' responses centered on the DOD's Joint Tactical Radio (JTR) program[34] as an example of how the DOD is addressing the interoperability dilemma. Although this discussion offered some comfort to Senator Robb, it fell short of offering a clear answer to his question of how to reconcile the age-old procurement and interoperability issue in light of the DOD's new information superiority goal. The hearing did not touch on the services' view that they cannot wait for the JTR program to deliver a joint capability but must have an interim capability immediately. As of mid-1998, the services were acquiring a limited number of service-unique radios.[35] Whether the approach of fielding limited numbers of these until joint radios become available will create further interoperability problems remains to be seen, but heralding this example as an approach to remedying the DOD's thirty-year-old interoperability problems is unconvincing.

Such questions are not new. Neil Munro, who provides current C^4I analysis for *Defense News*, complimented the DOD on interoperability in *The Quick and the Dead* (1991), his study of electronic combat and modern warfare. Writing this book while forces massed for Desert Storm, Munro gave the DOD credit for having made great strides in the area of interoperability but cautioned that the DOD "must always strive to control the separatist tendencies of its various services and communities, who will seek to build C^3I systems that suit their purposes, but not the purposes of other services or the DOD."[36]

The GAO, probably the toughest critic of the DOD's ability to field interoperable C^4ISR systems, has reports that go back ten and more years which document consistent problems with the way the DOD fields common and compatible C^3 equipment. A sample survey of findings in GAO reports revealed a long-held view of the need for interoperability among C^3 systems while seeming also to suggest a lack of commitment in the DOD to a long-term strategy that would be supported by resources adequate to achieving it. The GAO's findings, bluntly stated, were highly critical of the DOD's approach to achieving interoperability among C^4I systems, and, without change in the DOD's practice, future surveys of GAO reports would yield predictable results.

For example, *Joint Military Operations: Weaknesses in DOD's Process for Certifying C^4I Systems' Interoperability*, the most recent GAO report (1998), declared, among other things, that the DOD's process for certifying existing, newly developed, and modified C^4ISR systems for interoperability was inadequate.[37] A 1993 GAO report, *Joint Military Operations: DOD's*

---

[34]For a description of the Joint Tactical Radio (JTR) program, the DOD's effort to consolidate the services' programmable, modular, tactical radio development and acquisition programs into a single program, see Edward J. Walsh, "Joint Tactical Radio Spurs Rapid Technology Insertion," *Signal Magazine* **52**, 8 (April 1998), 67-70.

[35]U.S. GAO/NSIAD, *Defense Information Superiority: Progress Made, but Significant Challenges Remain* (Washington, D.C.: GAO/NSIAD/AIMD-98-257, August 1998), 4.

[36]Neil Munro, *The Quick and the Dead* (New York: St. Martin's Press, 1991), 77.

[37]U.S. GAO/NSIAD, Joint Military Operations; Weaknesses in the DOD's Process for Certifying C^4I Systems' Interoperability (Washington, D.C.: GAO/NSIAD-98-73, March 1998), 2.

Renewed Emphasis on Interoperability Is Important but Not Adequate, stated that the services tend "to develop their own C4I systems independent of one another without consideration for joint requirements,"[38] which it gave as the primary reason for the lack of interoperability. Last, a 1987 report, *Interoperability: DOD's Efforts to Achieve Interoperability Among C3 Systems*, gave some indication of how long these issues have been around by providing testimony that showed that "the services have been unable to communicate effectively among themselves during joint operations and exercises… [T]his was the case in Korea, the Dominican Republic landing, Vietnam and, almost twenty years later, during the Grenada intervention in 1983."[39] The report went on to present a scenario whereby the DOD was unable, until 1985, to update a 1967 version of DOD Directive 4630.5, on interoperability policies and procedures for C3 equipment, owing to disagreements among the services.

As an aside, the DOD is currently in the process of attempting to update its 1992 interoperability directive (DOD Directive 4630.5) with a 1998 version titled *Information Interoperability*.[40]

The shortcomings in the DOD's interoperability process reported by the GAO and others over the years cannot be resolved here, but, just as plans for achieving information superiority are on the drawing board, this report offers some modest suggestions on how the DOD might enhance C4ISR interoperability. The author does this because he believes that, without C4ISR systems interoperability, information superiority will come, if it can indeed be achieved, only at a very high price.

2.5 Expectations

Information superiority has captured the imagination of past and present leaders of the DOD. The stakes are high, and the circumstances in which success must be achieved keep changing. Additional fiscal resources for C4ISR are not an option, according to Secretary Cohen's message in the 1997 QDR, but achieving information superiority remains a high priority in the DOD, for reasons the Secretary and General Shalikashvili both expressed.

According to Secretary Cohen, the Department is committed to achieving information superiority[41]:

---

[38]U.S. GAO/NSIAD, *Joint Military Operations: DOD's Renewed Emphasis on Interoperability Is Important but Not Adequate* (Washington, D.C.: GAO/NSIAD-94-47, October 1993), 1.

[39]U.S. GAO/NSIAD, *Interoperability: DOD's Efforts to Achieve Interoperability Among C3 Systems* (Washington, D.C.: GAO/NSIAD-87-124, April 1987), 8.

[40]See unpublished draft of Department of Defense, *Information Interoperability*, Directive 4630.5 (Washington, D.C.: The Pentagon, January 1998).

> the overall advantages of achieving information superiority are expected to be increasing speed of command, enabling forward deployed and early-entry forces to take the initiative away from numerically superior enemy forces and set the conditions for early, favorable termination of a conflict.[42]

And in *Joint Vision 2010* General Shalikashvili stated that

> information superiority and advances in technology will enable us to achieve the desired effects through the tailored application of joint combat power…to accomplish the effects of mass—the necessary concentration of combat power at the decisive time and place—with less need to mass forces physically than in the past.[43]

The DOD thus appears committed to developing C^4ISR capabilities that will achieve information superiority. Secretary Cohen and General Shalikashvili might agree that, with new technologies emerging from the information age, future military operations may be carried out very differently from those of the past, even the recent past. According to Admiral Jay Johnson, "the battlefield of the 21st Century will be one in which the force with the mastery of the information spectrum will prevail."[44]

---

[41]William S. Cohen, Secretary of Defense, "Transforming U.S. Forces for the Future," Section VII, *Report of the Quadrennial Defense Review* (Washington, D.C.: Pentagon, May 1997), [On-line]. URL: <http://www.defenselink.mil/pubs/qdr/sec7.html> (Accessed March 9, 1998.)

[42]Ibid.

[43]Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Pentagon, 1996), 17-18.

[44]Jay L. Johnson, "Speech to the Current Strategy Forum at the Naval War College in Newport, R.I., June 12, 1997," [On-line]. URL: <http://www.chinfo.navy.mil/navpalib/people/flags/johnson_j/speeches/stratfor.txt> (Accessed Sept. 4, 1997.)

Chapter Three
Information Superiority: Capability, Ability, or Condition?

> *Any military—like any company or corporation—has to perform at least four key functions with respect to knowledge. It must acquire, process, distribute, and protect information, while selectively denying or distributing it to its adversaries and/or allies.*[1]

This chapter traces the term "information superiority" to its origins in the DOD and presents various interpretations of it to show how the term evolved from the C^{4}I for the Warrior vision and how both it and the ideas it embodies have developed. The chapter takes issue with the view of information superiority as either a capability or an ability and suggests why something altogether different is necessary to describe what information superiority consists of and means.

3.1 Information Superiority and the C^{4}IFTW Vision

Although the first published use by the DOD of the term "information superiority" appeared in *C^{4}I for the Warrior: A 1995 Progress Report*[2] (see **Figure 3-1**), the idea goes back as far as the 1992 *C^{4}I for the Warrior*[3] vision, which was conceived by the Joint Staff as a result of the C^{4}I experiences of the Persian Gulf war (1990–91) and promulgated as a document in 1992. The theme of *C^{4}I for the Warrior* was the interoperability of C^{4}I systems to meet the needs of future warriors by providing

> a fused, real time, true representation of the warrior's battlespace—an ability to order, respond and coordinate horizontally and vertically to the degree necessary to prosecute [the] mission in that battlespace.[4]

The plan to meet this goal was described as three-phased:

1. **Quick-Fix Phase (Program Objective Memorandum [POM] Years):** Installation of translation devices that interpret nonstandard message and data formats and protocols

2. **Mid-Term Phase (POM Plus Ten Years) Concurrent with the Quick-Fix Phase:** Development of a global C^{4}I system capable of generating and delivering fused information

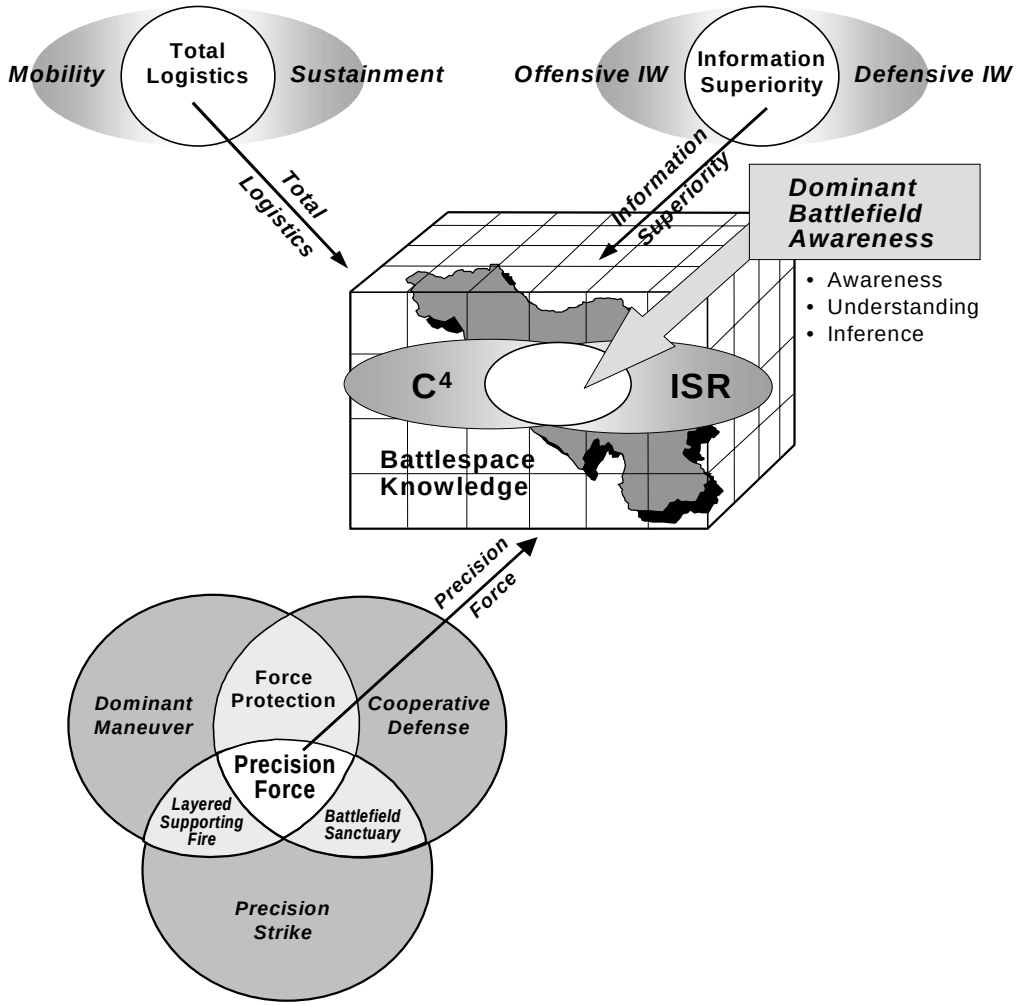
---

[1]Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 141-142.

[2]Office of the Director for C^4 Systems, The Joint Staff, *C^{4}I for the Warrior: A 1995 Progress Report* (Washington, D.C.: The Pentagon [early 1996]), 4-5.

[3]Office of the Director for C^4 Systems, The Joint Staff, *C^{4}I for the Warrior* (Washington, D.C.: The Pentagon, June 12, 1992), [n.p.].

[4]Ibid., [16-17].



C4ISR = command, control, communications, computers and intelligence, surveillance, and reconnaissance
IW = information warfare

Source: Office of the Director for C4 Systems, The Joint Staff, *C4I for the Warrior: A 1995 Progress Report* (Washington, D.C.: The Pentagon, [early 1996]), 5.

Figure 3-1

"System of Systems": Dominating the Joint Battlespace

3. **Objective Phase (Extended beyond Year 2000):** Dependent on advanced technology drivers, such as artificial intelligence (AI) applications, multilevel security, data compression and data fusion, and common operating and interface environments.[5]

Updated annually, by 1995 the C4IFTW vision document had become less a vision than an annual report on C4I initiatives. Although the title implies both C4 and I, the vision is concerned far more

[5]Ibid.

with C^4 than I. In early 1996, information superiority was not the target of much attention and no particular meaning for the term was provided in the publication, which simply asserted that

> information superiority will enable our forces to know where they are and where the opponent is; to see the battlespace and command while denying our opponent the ability.[6]

As expected, this assertion supported the original goals of the 1992 C^4IFTW vision, but it also raised the question of whether information superiority is what will enable U.S. forces to know where they are and where the opponent is or whether it is what is derived from the DOD's network of C^4ISR systems. In this report information superiority is taken to mean the latter, that is, that information superiority is achieved through effective information operations that use protected, integrated, and interoperable C^4ISR systems.

In the most recent update of the C^4IFTW vision, published in January 1998, information superiority was more prominent than in the 1996 publication. The 1998 update sees information superiority as the "objective goal"[7] of the C^4IFTW vision. The inside cover shows the pictures and signatures of the Pentagon's senior military C^4 professionals,[8] implying a declaration achieved by consensus. Yet in the same document each military service described its path toward information superiority just slightly differently. For example, in the view of the Joint Staff, in harmony with *Joint Vision 2010*, information superiority is "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[9] At the same time, the Army maintains that "digitization will enable the Army of the 21st Century to achieve information superiority."[10] And the Navy and Marine Corps state, among other things, that "the most important facet of information superiority, whether in support operations or in combat, is time."[11] Last, the Air Force views information superiority as "the enabling core competency for all other Air Force capabilities."[12] This approach, of simply

---

[6]*C^4I for the Warrior: A 1995 Progress Report*, 4.

[7]Office of the Director for C^4 Systems, Joint Chiefs of Staff, *C^4I for the Warrior: The Joint Vision for C^4I Interoperability* (Washington, D.C.: The Pentagon, January 1998), 20.

[8]Ibid., ii: Lt. Gen. Douglas D. Buchholz, USA, Director. Command, Control, Communications, and Computer Systems, The Joint Staff; and Lt. Gen., William H. Campbell, USA, Director of Information Systems for Command, Control, Communications, and Computers, United States Army; Vice Admiral, USN, Arthur K. Cebrowski, Director, Space, Information Warfare, Command and Control, United States Navy; Maj. Gen. USMC, Joseph T. Anderson, Assistant Chief of Staff, Command, Control, Communications, Computers, and Intelligence [United States Marine Corps]; and Lt. Gen. USAF, William J. Donahue, Deputy Chief of Staff, Communications and Information, United States Air Force.

[9]Ibid.

[10]Ibid., 21.

[11]Ibid.

[12]Ibid.

publishing each service's interpretation of information superiority, could have profound doctrinal implications and suggests a certain unwillingness to force conformance.

A more challenging approach to outlining a joint vision for C^4I interoperability might have been to apply the then approved meaning of information superiority—"that degree of dominance in the information domain which permits the conduct of operations without effective opposition" [13]—and focus the C^4IFTW vision on developing information operations. In this way, the Joint Staff might have developed its vision for C^4I interoperability to emphasize future military operations to be conducted by a joint force operating with greatest effectiveness by means of integrated C^4ISR systems designed for this purpose.

3.2. The Uses of Information Superiority

Even as it became increasingly evident in 1995 that more attention needed to be put toward interoperability,[14] Admiral Owens started to push for integration of C^4ISR systems. Vice-Admiral Cebrowski, then the Joint Staff Director for C^4 Systems, used the illustration shown in **Figure 3-1** to suggest the possibility of integrating the myriad C^4ISR systems into an emerging "system of systems."[15] Through this vision, shared by Admiral Owens, then Vice-Chairman of the Joint Chiefs of Staff, the notion of information superiority began to be applied in the Joint Staff.

Information superiority made its debut in joint doctrine with the definition of information warfare in *Joint Doctrine for Command and Control (C^2) Warfare*, Joint Publication 3-13.1:

> Information Warfare is defined as actions taken to achieve *information superiority* [emphasis added] by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.[16]

---

[13]*Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: The Pentagon, March 23, 1994), [On-line]. URL: <http://www.dtic.mil/doctrine/jel/doddict/> (Accessed Jan. 15, 1999.)

[14]This passage refers to a study sponsored by the Joint Staff and conducted in 1995 that revealed that of 424 acquisition managers and students at the Defense Systems Management College surveyed only 12 (less than 3 percent) knew about the DOD's interoperability requirements related to C^4 systems. See GAO/NSIAD, *Joint Military Operations; Weaknesses in DOD's Process for Certifying C^4I Systems' Interoperability* (Washington, D.C.: GAO/NSIAD-98-73, March 1998), 6.

[15]See William A. Owens, "The Emerging System of Systems," *U.S. Naval Institute Proceedings* **121**, 5 (May 1995), 35-39.

[16]*Joint Doctrine for Command and Control Warfare*, Joint Publication 3-13.1 (Washington, D.C.: The Pentagon, Feb. 7, 1996), I-3.

This use of the term information superiority supports the argument here that information superiority is not "the *capability* to collect, process and disseminate"[17] or "the *ability* to collect and distribute"[18] nor even "the first *function* of the Air Force"[19] but a *condition* achieved through information operations enabled by C^4ISR systems that are protected, integrated, and interoperable.

But the Joint Staff, the services, or agencies none of them claim to have invented the term and so should not bear sole responsibility for its vague application.

In 1993, in *War and Anti-War*, Alvin and Heidi Toffler wrote that "at least some wars can now be won with information superiority,"[20] and posed the question, "can anti-wars be won that way too?"[21]

In 1995, in the "The Challenge of Information Warfare," Major General Wang Pufeng, former Director of the Strategy Department at the Academy of Military Science in Beijing, noted that "firepower superiority depends on information superiority."[22] Exploring there the notion of information weapons systems and their potential, General Wang advocated strengthening China's military through information technology and the "use of information superiority to achieve greater victories at a smaller cost."[23]

The discussion so far has shown that, for the moment, achieving information superiority means different things to different people and suggests that reconciling the divergent views may prove difficult, because many of the principals or their predecessors have taken public positions to which their staffs now simply refer.

Information superiority was a central precept of General Shalikashvili's *Joint Vision 2010*,[24] to combine, according to Lt. General Buchholz, "the exploitation of information and the lethality

---

[17]Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: The Pentagon [1996]), 16.

[18]William S. Cohen, Secretary of Defense, in "What's New?" in the "The Secretary's Message," *QDR* (Washington, D.C.: The Pentagon, May 1997), [On-line]. URL: <http://www.defenselink.mil/pubs/qdr/msg.html> (Accessed March 10, 1998.)

[19]*Air Force Doctrine*, Air Force Doctrine Document 1 (Washington, D.C.: The Pentagon, September 1997), 31.

[20]*War and Anti-War*, 230.

[21]Ibid.

[22]Maj. Gen. Wang Pufeng, "The Challenge of Information Warfare," *China Military Scienc*e (Spring 1995), cited in *Chinese Views of Future Warfare*, edited by Michael Pillsbury (Washington, D.C.: NDU Press, 1997), 318.

[23]Ibid.

[24]*Joint Vision 2010*, 17.

of precision weapons to become a formidable combat force multiplier."[25] On joint military operations, General Shalikashvili saw that the United States "will require more than just an [information] edge over an adversary" but must have information superiority.[26] He suggested a variety of methods for attaining information superiority, some traditional combat operations, such as an attack on an adversary's C^2 capability, and some so-called information operations, such as electronic intrusion to degrade or exploit an adversary's C^2 system. *Joint Vision 2010* implied that the DOD will need either to elevate the priority of advancing and modernizing C^4ISR systems or to reform the existing C^4ISR modernization process to produce protected, integrated, and interoperable C^4ISR systems.

Other DOD leaders echoed *Joint Vision 2010*, adopting General Shalikashvili's meaning, or a variation on it, for information superiority and incorporating it into their own speeches and vision documents. Lt. General Kenneth A. Minnihan, then Director of the National Security Agency (NSA), for example, included information superiority in his strategic plan for the twenty-first century, in which, citing *Joint Vision 2010*, he declared information superiority the United States's new national effort.[27] In "C^4IFTW: Teamwork for the Warrior," Lt. General Albert J. Edmonds, USAF, Ret., a former Director of the DOD's Information Systems Agency, considered information superiority vital to the armed forces but varied slightly from the meaning offered in *Joint Vision 2010* in regarding it as "the ability to collect, process and disseminate an uninterrupted flow of information while denying our enemy that ability."[28]

In *Army Vision 2010*, General Dennis J. Reimer, Chief of Staff of the Army, included information superiority as something the Army must have, and, like General Shalikashvili, described it as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[29] The Chief of Naval Operations, Admiral Jay Johnson, embraced information superiority as part of his network-centric warfare vision, believing that it would provide a clearer view of the battlespace. For example, in remarks presented to the Current Strategy Forum in Newport, Rhode Island, Admiral Johnson, relating information superiority to Clausewitz's "fog" and "friction,"[30] stated that "information superiority by definition helps reduce friction by clearing away that fog of war. It

---

[25]Cited in Lt. Gen. Douglas Buchholz, "Joint Dominance," *Military Information Technology* **1**, 3 (October–November 1997), 16.

[26]*Joint Vision 2010*, 16.

[27]National Security Agency, National Cryptologic Strategy for the 21st Century (June 1996), [On-line]. URL: <http://www.nsa.gov:8080//programs/ncs21/director.html> Accessed Jan. 30, 1998.)

[28]Lt. Gen. Albert J. Edmonds, "C^4IFTW; Teamwork for the Warrior," *Defense* **97**, 2 [1997], 22.

[29]Department of the Army, *Army Vision 2010* (Washington, D.C., November 1996), [On-line]. URL: <http://www.army.mil/2010/information_superiority.htm> (Accessed Jan. 22, 1998.)

[30]Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 117-121.

will enable us to win, and win decisively."[31] And in 1997, Sheila Widnall, the former Secretary of the Air Force, and General Ronald R. Fogleman, USAF, Ret., the former Chief of Staff of the Air Force, together expressed support for information superiority as an Air Force core competency, an "ability to collect, control, exploit and defend information while denying the adversary the same" and viewed it as "critical to ensuring successful military operations in the future."[32]

In April 1996, a blue-ribbon panel commissioned by the Director, National Reconnaissance Office (NRO), and chaired by Admiral David Jeremiah, USN, Ret., former Vice-Chairman of the Joint Chiefs of Staff, was formed to review the NRO's mission and business practices and to make recommendations regarding its role in the twenty-first century. The panel enthusiastically embraced the notion of information superiority, even recommending that "the NRO should be responsible for the unique and innovative technology, large-scale systems engineering, development and acquisition, and operation of space reconnaissance systems and related intelligence activities needed to support global information superiority."[33]

3.3 Information Superiority: A Condition

One of the three goals here (see section **3.5**) is to clarify the meaning and usage of "information superiority," because a common understanding is useful for the remainder of this report and may help, generally, in ascertaining whether information superiority has been achieved. It is suggested here that information superiority may be usefully viewed as a condition that can be achieved through effective information operations enabled by C^4ISR systems.

Hair-splitting has an air of the pedantic, yet there is an important distinction to be made here, not between *ability* and *capability*, which mean much the same thing and have the same linguistic root, but between both those terms and *condition*. Ability and capability both signify possession of the necessary power, resources, and skill to carry out a project; both depend on being "able," whether now or potentially. Condition refers instead to a mode or state, to a premise on which the fulfillment of an agreement or a course of action depends. Here the term *condition* is used to mean that which planners and warriors need to achieve—such as information superiority—as a basis for deciding further action, and achieving that condition requires the use of C^4ISR *capabilities*—the necessary power, resources, and skill in gathering and assessing information and intelligence—to gain an operational advantage and minimize the risks of an

---

[31]Jay L. Johnson, "Speech to the Current Strategy Forum at the Naval War College in Newport, R.I., June 12, 1997," [On-line]. URL: <http://www.chinfo.navy.mil/navpalib/people/flags/johnson_j/speeches/stratfo.txt> (Accessed Sept. 4, 1997.)

[32]Department of the Air Force, *Air Force Issues Book 1997*, Air Force Core Competencies, Information Superiority, [On-line]. URL: <http://www.af.mil/lib/afissues/1997/issues28.html> (Accessed July 7, 1998.)

[33]Final Report the Director, NRO, Defining the Future of the NRO for the 21st Century (Aug. 26, 1996), [On-line]. URL: <http://www.nro.odci.gov/jpanel/jersum.html#issue2> (Accessed July 7, 1997).

overall campaign. (The Scale of Information Domain Conditions, discussed in section **4.2.1**, rests on this meaning of condition.)

The *condition* is that degree of dominance in the information domain that permits the conduct of operations without effective opposition.[34]

Information operations are actions taken to affect adversary information and information systems while defending one's own information and information systems.[35]

The *capability* consists of a network of protected, integrated, and interoperable C^4ISR systems that provide joint warriors with timely, reliable, and relevant information to the right place, in time allowing forces to seize the opportunity and meet the objectives across the full range of military operations.[36]

---

[34]*Department of Defense Dictionary of Military and Associated Terms.*

[35]*Joint Doctrine for Information Operations*, Joint Publication 3-13 (Washington, D.C.: The Pentagon, Oct. 9, 1998), GL-7.

[36]See *Doctrine for Command, Control, Communications, and Computer (C^4) Systems Support to Joint Operations*, Joint Publication 6-0 (Washington, D.C.: The Pentagon, May 30, 1995), I-1.

Chapter Four
The Information Domain

> *Therefore I say: Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.*[1]

This chapter attempts to move information superiority from the theoretical realm to the practical. It is devoted to the development of a six-point scale—from information inferiority, disadvantage, parity, to advantage, superiority, and supremacy—that may be used to identify information domain conditions.

4.1 Information and the Chaos of War

Before attempting either to develop a scale for the information domain or to determine whether information superiority can be measured, some reflections on war may help provide some perspective. Clausewitz, writing on war, said its nature was "slaughter and its price…blood."[2] Information superiority is unlikely to change the nature of war or eliminate the need for it. But devotees of Sun Tzu are encouraged to speculate that achieving information superiority during military operations might result in success without a fight:[3] were a commander to recognize that an opposing force had achieved information superiority whereby it controlled the information domain and denied the commander the ability to direct forces, the commander would have to be resigned to admitting defeat.

Then is it conceivable that future C^{4}ISR systems might be so capable that they could eliminate the usual chaos associated with war? Frank M. Snyder, the Raymond A. Spruance Professor of Command and Control (Emeritus) of the Naval War College, seems not to think so. According to Snyder, in *Command and Control: The Literature and Commentaries*,

> the uncertainties that surround [the information commanders need to assess a situation] are many: the information available is usually incomplete, conflicting, or ambiguous; it often arrives late, after having

---

[1]Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London, Oxford, New York: Oxford University Press, 1963), 84.

[2]Carl von Clausewitz, *On War,* translated and edited by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 259.

[3]"For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill." See Sun Tzu, *The Art of War*, 77.

> been transmitted imperfectly or received with error; and it may be misunderstood or misinterpreted.[4]

This view coincides with Clausewitz's: "reports in war are contradictory," he wrote in *On War*, in a chapter on intelligence, "even more are false, and most are uncertain."[5]

While some have come to believe that information age technologies may ultimately pierce the fog of war, others steadfastly maintain the opinion that the fog will persist. Frank Snyder offered an interesting analogy: "why—with the near universal access to financial information—some people continue to lose money in the stock market while others are making a great deal of it."[6]

4.2 Information Superiority in an Operational Context

In **Chapter Three** the reader was invited to consider information superiority as a condition much like air and maritime superiority.[7] As a condition like them, information superiority can be plotted as one of six points on a scale of information domain conditions (see **Figure 4-1**), similar to the scale of Defense Readiness Conditions (DEFCON).[8] This chapter attempts to move information superiority from the theoretical realm into the practical. The scale and the associated definitions, discussed below, include six conditions with an explanation, or definition, of what each means. These definitions may be useful for placing information superiority into a theoretical context and necessary also because of the wide use of information superiority to mean, variously, a "capability to collect, process and disseminate"[9] or an "ability to collect and distribute"[10] (see section **1.1** and **Chapter Three**).

---

[4]See Frank M. Snyder, *Command and Control: The Literature and Commentaries* (Washington, D.C.: NDU Press, INSS, 1993), 28.

[5]Clausewitz, 117.

[6]Personal communication by Frank M. Snyder to Anthony G. Oettinger, Nov. 23, 1998.

[7]*Joint Warfare of the Armed Forces of the United States*, Joint Publication 1, 2nd ed., using the Persian Gulf crisis and conflict of 1990–91 as an example, describes how gaining air superiority and maritime superiority were preconditions for further operations. See *Joint Warfare of the Armed Forces of the United States*, 2nd ed., Joint Publication 1 (Washington, D.C.: The Pentagon, Jan.10, 1995), Appendix A, A-3, [On-line]. URL: <http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf> (Accessed March 12, 1998.)

[8]Defense Readiness Conditions: A uniform system of progressive alert postures for the use between the Chairman of the Joint Chiefs of Staff and the commanders of unified commands and for use by the services. Defense readiness conditions are graduated to match situations of varying military severity (status of alert). Defense readiness conditions are identified by the short title DEFCON (5), (4), (3), (2), and (1), as appropriate. See *Department of Defense Dictionary of Military and Associated Term*s, Joint Publication 1-02 (Washington, D.C.: The Pentagon, March 23, 1994), [On-line]. URL: <http://www.dtic.mil/doctrine/jel/doddict/> (Accessed June 25, 1998.)

[9]Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: The Pentagon, 1996), 16.

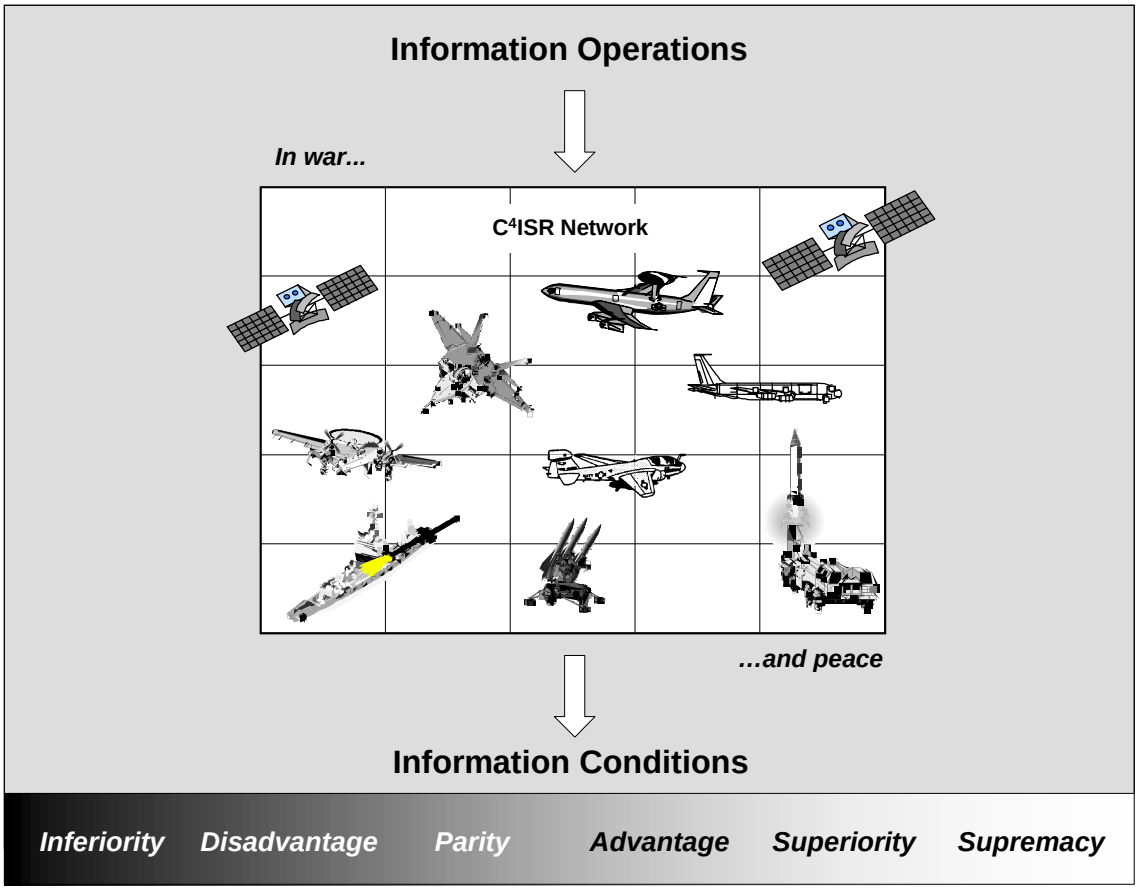


Figure 4-1

Scale of Information Domain Conditions

4.2.1 Scale of Information Domain Conditions

Of the six terms shown below, information superiority is the only one to have an approved meaning in the *Department of Defense Dictionary of Military and Associated Terms*,[11] one that has undergone an extensive coordination process that included the Office of the Secretary of Defense, the Joint Staff, the services, and Defense agencies, leading to approval by the DOD in mid-1997. By October 1998, even that definition had been superseded, by approval of Joint

[10]William S. Cohen, Secretary of Defense, in the section on "What's New?" of "The Secretary's Message" in *Report of the Quadrennial Defense Review* (Washington, D.C.: The Pentagon, May 1997), [On-line]. URL: <http://www.defenselink.mil/pubs/qdr/msg.html> (Accessed March 10, 1998.)

[11]Joint Publication 1-02 (Washington, D.C.: The Pentagon, March 23, 1994), [On-line]. URL: <http://www.dtic.mil/doctrine/jel/doddict/> (Accessed Jan. 15, 1999.)

Publication 3-13, *Joint Doctrine for Information Operations* (see section **1.1**).[12] In spite of this effort, the term is still used varyingly, and usages are unclear and sometimes misleading.

The other five terms used on the scale have been developed to support one goal of this report, namely, to ascertain whether information superiority can be measured by assessing the performance of C^4ISR systems during military operations. A literature search showed that the terms "information advantage"[13] and "information parity,"[14] both used here, have been used sparingly in the professional literature; and the same search discovered only two uses of the term "information supremacy."[15] The remaining terms, "information disadvantage" and "information inferiority," were not found in any of the published material read as part of the research for this report.

The following are definitions of the terms on the scale of the information domain conditions (**Figure 4-1**):

- *Information Inferiority*—That degree of suppression in the information domain that persistently denies the conduct of operations due to absolute effective opposition.
- *Information Disadvantage*—That degree of suppression in the information domain that denies the conduct of operations due to effective opposition.
- *Information Parity*—The condition in the information domain that permits the conduct of operations with functional equivalence by all.
- *Information Advantage*—That degree of dominance in the information domain that permits the conduct of operations with relatively minor opposition.

---

[12]The new definition was approved, on Oct. 9, 1998, with approval of *Joint Doctrine for Information Operations*, Joint Publication 3-13 (Washington, D.C.: The Pentagon, Oct. 9, 1998), GL-7.

[13]Raymond C. Bjorklund uses the term information advantage in *The Dollars and Sense of Command and Control* (Washington, D.C.: NDU Press, INSS, 1995), 89-95; Thomas G. Mahnken writes of achieving an information advantage in "War in the Information Age," *Joint Force Quarterly*, 10 (Winter 1995–96), 41.

[14]The Electronic Industries Association, in "EIA Foresees Major Market and High Hurdles in Information Superiority," (Oct. 9, 1997), a press release, reported "that simplifying the rules to speed buying of commercial items will get the United States to information parity and save money needed to develop the military technologies needed for superiority." See [On-line]. URL: <http://www.eia.org/pad/press/files/9710/97-62.htm> (Accessed April 17, 1998.) Charles J. Dunlap, Jr., used the term "information parity" in "*Joint Vision 2010*: A Red Team Assessment" (*Joint Force Quarterly*, 17 [Autumn–Winter 1997-98], 49): "We should prepare to fight in the more realistic environment of information parity, which would also have the benefit of even greater dominance should information superiority somehow be achieved."

[15]"Information supremacy" appeared as part of the "Vision" of the Office of the Director for C^4 Systems, Joint Chiefs of Staff: "We are teamed with the CINCs, Services, Agencies and Industry to advance and protect the Nation's information supremacy." See [On-line]. URL: <http://www.dtic.mil/jcs/j6/vision.html> [Home page] (Accessed June 5, 1998.) Dunlap, in "*Joint Vision 2010*: A Red Team Assessment," also used the term "information supremacy": "Therefore it is troubling that *JV2010* appears to be so dependent upon information supremacy" (49).

- *Information Supremacy*—That degree of dominance in the information domain that permits the conduct of operations without any opposition and totally denies an adversary the use of the information domain.

4.3 Theory versus Practice

Once embarked on a mission, commanders and the "information warriors" who support them would have little time to devote to fine points of the scale of the information domain introduced here. They would be too busy trying to figure out how to use protected, integrated, and interoperable C^4ISR systems to attain information superiority, how to conduct information operations to gain and maintain such superiority, and how to accomplish the objectives assigned to them as part of an overall campaign. To do all this, commanders would need to know *how* to attain information superiority during military operations, yet at the writing of this report no such "how-to" guidance was available. Policymakers and writers of doctrine might start to fill this void by developing a set of joint unifying principles for information operations, with the explicit goal of achieving information superiority,[16] as well as developing joint tactics, techniques, and procedures[17] to describe how C^4ISR systems might be employed to achieve it.

4.3.1 Moving from the Theoretical

Whether the theoretical and practical aspects of information superiority can be bridged may be worth exploring. Put another way, why did not past commanders of military operations talk of achieving information superiority? An explanation may reside in an analogy to achieving air superiority.[18] Benjamin Franklin Cooling, in *Case Studies in the Achievement of Air Superiority*, which traces some of the history related to air superiority prior to World War II, cited an

---

[16]The Joint Staff and the departments of the Army and Air Force have already begun to write doctrine on information operations. The first draft of *Joint Doctrine for Information Operations*, Joint Pub. 3-13 (Washington, D. C., Jan. 21, 1997) treated information superiority as "the capability to collect, process…." *Information Operations*, Dept. of the Army FM 100-6 (Washington, D.C.: The Pentagon, Aug. 27, 1996), 6-15, treats information superiority as something commanders leverage "to employ weapons systems, including joint assets" and as a term to define other terms; see 1-9 and 2-2, [On-line]. URL: <http://www.atsc-army.org/cgi-bin/atdl.dll/fm/100-6/toc.htm> (Accessed March 25, 1998.) In *Information Operations* (Washington, D.C.: The Pentagon, Dept. of the Air Force draft of AFDD 2-5, December 1997) information superiority is treated as an enabling function; see [On-line]. URL: <http://www.hqafdc.maxwell.af.mil/> (Accessed March 25, 1998.)

[17]See *Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program*, Joint Publication 1-01 [with Change 1] (Washington, D. C.: The Joint Staff, Sept. 14, 1993), I-1.

[18]For a discussion of how superiority in information technology can be used as an element of national power, see Richard M. Jensen, *Information War Power: Lessons from Air Power* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-97-2, September 1997), in which Jensen offers a contextual framework for the development of information policy by comparison to a historically familiar frame of reference, issues surrounding the development of air power and strategic bombing doctrine that arose between the world wars.

American flyer as remembering that "during that period, we really didn't know what we were trying to do. We were doing it but not defining it."[19]

In the past, commanders of military operations may have acted intuitively to achieve information superiority, without defining what they were after. Or they may have relied on their technical staffs to achieve it, without directly specifying information superiority as an objective. Generally, they probably did not get into the nuts and bolts of the C^4ISR systems, as they are now collectively known, on which they relied, unless, of course, a system failed to provide the products advertised, suffered unexplained circuit outages or software crashes, or experienced a shortage of parts for repair, causing unacceptable systems outages.

But such passive involvement by commanders is changing. Vulnerabilities associated with dependence on C^4ISR systems, coupled with the emergence of new information-age capabilities, such as software to detect electronic intrusions, have begun to increase commanders' consciousness of this new information aspect of warfare. Commanders in the not so distant future may attribute part of their successes to having achieved information superiority, much as—to return to the analogy to air superiority—General Dwight D. Eisenhower, attributed his success in the invasion of Normandy to "air supremacy": "riding through Normandy after D-Day, [he] remarked to his son, 'If I didn't have air supremacy, I wouldn't be here.'"[20]

Whether or not a commander had achieved air superiority has not always been clear. Air power experts struggled with this issue during and after World War II. Cooling and others report on the various interpretations of air superiority in *Case Studies in the Achievement of Air Superiority*, and according to Cooling:

> some observers have interpreted air superiority as the possession of a larger air force, or one which has greater destructive power. Others have seen it as the ability to drive the enemy air force onto the defensive and thus deny the opposition the means of carrying out counteroffensive operations.[21]

For others, air superiority is the "ability to fly at will over enemy territory, and to some extent prevent the enemy from doing the same."[22] Agreement must have been reached at some point, because today no one would challenge the assertion that in Desert Shield/ Desert Storm, for example, air superiority was achieved.

---

[19]Benjamin Franklin Cooling, "Introduction," *Case Studies in the Achievement of Air Superiority* (Washington, D.C.: Center for Air Force History, Special Studies, U.S. Gov't Printing Office, 1991; reprt. 1994), xvi.

[20]Ibid., Richard P. Hallion, "Foreword," iii.

[21]Ibid., Cooling, "Introduction," xvi.

[22]Ibid., citing Sir Charles Webster and Noble Frankland, *The Strategic Air Offensive Against Germany, 1939–1945: United Kingdom History of the Second World War* (London: H. M. Stationery Office, 1961), 20-23.

The same seems to hold true for maritime superiority. Maritime experts appear comfortable knowing they achieved maritime superiority in Desert Shield/Desert Storm. Afterward, the Pentagon reported that "the Persian Gulf War demonstrated once again that sea control is fundamental to successful power projection, and revalidated the importance of maritime superiority to US global leadership."[23] Detailing the campaign, the Pentagon further elaborated that "as a first order of business, the campaign fought for and gained air superiority and maritime superiority as preconditions for further operations."[24]

But whatever makes commanders comfortable with knowing that they have achieved air and maritime superiority, there seems to be something different, something less tangible, in knowing if and when one has achieved information superiority. According to Alan Campen, there are significant differences between information superiority and or maritime superiority. Air and maritime operations, according to him, involve conducting operations in "physical entities that can be identified, captured, and held. Ownership is not in doubt. Possession is exclusive. You know when you have achieved a condition of superiority in the physical realm."[25] Conducting information operations presents the commander with a variable not encountered in air or maritime operations, which is that "the same information can be mutually held: stolen, but still possessed by the owner."[26]

---

[23]U.S. Dept. of Defense, *Conduct of the Persian Gulf War,* Final Report to Congress (Washington. D.C.: The Pentagon, April 1992), 253.

[24] *Joint Warfare of the Armed Forces of the United States*, 2nd ed., Joint Publication 1 (Washington, D.C.: The Pentagon, Jan. 10, 1995), Appendix A, A-3, [On-line]. URL: <http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf> (Accessed March 12, 1998.)

[25]Personal communication by Alan D. Campen to Anthony G. Oettinger, July 5, 1998.

[26]Ibid.

Chapter Five

Can Information Superiority Be Measured?

This chapter attempts to answer the question of whether an information domain condition, that is, information superiority, can be measured by assessing the performance of C^4ISR systems in past military operations. Two joint operations now judged successful are examined in this light, the invasion of Grenada by U.S. forces in 1983[1] and the Persian Gulf conflict in 1990–91,[2] an international effort undertaken by a coalition forged for the particular occasion.

5.1 Urgent Fury

In the Spring of 1997, Congressman Duncan Hunter (Rep.-Calif.), Chairman of the Military Procurement Subcommittee, U.S. House of Representatives, 105th Congress, mentioned an episode from the successful invasion of Grenada in 1983 as he welcomed top C^4ISR officials from the Pentagon to a hearing on "Information Superiority for the 21st Century Battlefield." He then reminded those officials that he had not forgotten the less than stellar performance of the Pentagon's C^2 systems in the operation the Pentagon had dubbed *Urgent Fury*: "at one point," he said, "one of the Army commanders, to get some vital information, ended up putting a dime in the phone in Grenada and calling the Officers' Club at one of the bases back home."[3] That version of what happened in Grenada set the stage for the Information Superiority Hearings.

Although that version of events did not appear in the Pentagon's monograph titled *Operation Urgent Fury: Grenada*, the study does describe an incident, on October 27, 1983, when, in the Pentagon version, Army paratroopers "depended for fire support upon naval aircraft and naval gunfire."[4] According to Ronald Cole, the author of this study, because "their radios could not communicate with the ships of the Independence battle group, Army radiomen were forced to send their request for fire support to Fort Bragg which in turn relayed them by satellite to the ships."[5]

---

[1]For a complete discussion of the invasion of Grenada, beginning with the contingency planning for noncombatant evacuation after the coup on Oct. 12, 1983, which removed Grenada's Marxist leader, Maurice Bishop, and ending with the combat phase of operation Urgent Fury on Nov. 2, 1983, see Ronald H. Cole, *Operation Urgent Fury: Grenada* (Washington D.C.: Office of the Chairman of the Joint Chiefs of Staff, Joint History Office, 1997).

[2]For a complete discussion on the Persian Gulf war, see the U.S. Department of Defense, *Conduct of the Persian Gulf War*, DOD Final Report to Congress (Washington D.C: The Pentagon, April 1992).

[3]U.S. House of Representatives, Committee on National Security, "Information Superiority for the 21st Century Battlefield," *Hearings on National Defense Authorization Act for Fiscal Year 1998*, Joint Meeting of the Subcommittee on Military Procurement and the Subcommittee on Research and Development (Washington D.C.: U.S. Gov't Printing Office, March 20, 1997), 598.

[4]Cole, *Operation Urgent Fury: Grenada*, 51.

[5]Ibid., 51-52.

Other problems, which Congressman Hunter, did not mention, are described in the study, such as that "because of incompatible radios, Navy ships within sight of Rangers and airborne troops could not initially receive or respond to their requests for fire support. On two occasions, when Navy jets did respond, they attacked the wrong targets."[6]

Despite such shortcomings of the C^4ISR systems, operation Urgent Fury was a success. In January 1984, that is, soon after its conclusion, during a hearing on Capitol Hill on "Lessons Learned as a Result of the U.S. Military Operations in Grenada."[7] Admiral Wesley McDonald, USN, Ret., then Commander in Chief, U.S. Atlantic Command, called it a complete success. Nor was Admiral McDonald alone in his praise. Then Secretary of Defense Caspar Weinberger also felt that the operation in Grenada "went extremely well," while also admitting that "inevitably certain little things went wrong."[8]

By most accounts, it was a successful operation. It was successful even though C^2 systems interoperability problems were encountered. But was *information superiority* achieved during Urgent Fury? Colonel Raymond C. Bjorklund, USAF, Ret., in *The Dollars and Sense of Command and Control*, acknowledging that the initial C^2 system had some problems, Bjorklund concluded that "as the Urgent Fury C^2 system matured and stabilized in the early part of the conflict, the "information *advantage* [emphasis added]…leaned more toward the United States."[9]

Even though the information advantage went to U.S. forces in Urgent Fury, the effort fell short of reaching information superiority largely because of the interoperability problems in the C^2 systems that Bjorklund acknowledged. Without interoperable C^4ISR systems—that is, the ability of the many components of a network to interact with one another—U. S. efforts to achieve information superiority were (and will continue to be) stifled. C^4ISR systems interoperability is key to the quest for information superiority because, as said earlier (section **2.4**) without C^4ISR systems interoperability, information superiority will come, if it can indeed be achieved, only at a very high price. C^4ISR systems interoperability therefore needs to be considered in all its aspects when formulating joint unifying principles and joint tactics, techniques, and procedures for achieving information superiority.

---

[6]Ibid., 6.

[7]U.S. House of Representatives, Committee on Armed Services, *Full Committee Hearing on the Lessons Learned as a Result of the U.S. Military Operations in Grenada* (Washington, D.C.: U.S. Gov't Printing Office, Jan. 24, 1984), 15.

[8]U.S. Senate, Committee on Armed Services, *Reorganization of the Department of Defense Hearings Before the Committee on Armed Services*, S. Hrg. 99-1083, 99th Cong., 1st Sess., 1985 (Washington, D.C.: U.S. Gov't Printing Office, 1987), 118.

[9]Raymond C. Bjorklund, *The Dollars and Sense of Command and Control* (Washington, D.C.: NDU Press, INSS, 1995), 95.

5.2 Desert Shield/Desert Storm

Operation Desert Shield/Desert Storm is relevant to the topic of achieving information superiority for several reasons. First, this operation was, according to Alan D. Campen, "the first information war."[10] Second, it was characterized by Kenneth Allard as an operation that would be "remembered as the first war to demonstrate the means, the methods, and the awesome lethality of combat in the information age."[11] And, third, as this chapter was being written, in January 1998, U.S. and allied forces were staging for another operation in the Persian Gulf, one the Pentagon dubbed Desert Thunder, in response to Saddam Hussein's refusal to grant United Nations inspection teams unrestricted and unfettered access to suspected weapons storage sites allegedly containing weapons of mass destruction.

Did U.S. forces achieve information superiority during the 1990–91 Persian Gulf war? Even without stringent criteria for assessment, the answer initially appears to be a simple "yes." But would General Norman Schwarzkopf, USA, Ret., then Commander-in-Chief (CINC) of the U.S. Central Command, agree?

According to Joseph S. Toma, the C^4 network employed during Desert Shield/Desert Storm

> was the largest joint theater system ever established. It was built in record time and maintained a phenomenal 98 percent availability rate. At the height of the operation, the system supported 700,000 telephone calls and 152,000 messages per day [while] more than 30,000 radio frequencies were managed.[12]

The Pentagon's Final Report to Congress on the *Conduct of the Persian Gulf War* commended those who provided the logistical and technical base for the C^3 infrastructure and emphasized that the "ability to quickly disseminate information was testimony to the successful efforts of those"[13] responsible. The report further observed that the "overwhelming military victory against Iraqi armed forces was due in large part to accurate intelligence provided to decision makers, particularly at the national and theater level."[14]

---

[10]Alan D. Campen, "Introduction," *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*, edited by Alan D. Campen (Fairfax, Va.: AFCEA International Press, 1992), xx.

[11]Kenneth Allard, *Command, Control, and the Common Defense*, rev. ed. (Washington, D.C.: NDU Press, INSS, October 1996), 273.

[12]Joseph S. Toma, "Desert Storm Communications," in *The First Information War*, 1.

[13]Dept. of Defense, *Conduct of the Persian Gulf War*, Final Report to Congress (Washington D.C.: The Pentagon, April 1992), Appendix K, K-45.

[14]Ibid., Appendix C, C-17.

Although achieving information superiority was not an expressed goal in Desert Shield/ Desert Storm, it appears to have been a condition planners intuitively strove to achieve. U.S. and allied C^4ISR systems performed well, and much of Iraq's C^2 system was crippled. The Pentagon leadership expressed satisfaction in the Final Report and took the position that "C^3I in Desert Shield and Desert Storm was successful and may provide a model for future regional conflicts."[15] But what did the commander on the ground think?

On his return from Desert Shield/Desert Storm, on June 12, 1991, when General Schwarzkopf testified before the SASC, chaired by Senator Sam Nunn (Dem.-Ga.), he described some problem areas, specifically the need for an "immediately responsive intelligence capability that will give the theater commander near real time information that he needs to make decisions."[16] General Schwarzkopf recalled a talk with one of his subordinate commanders, Lt. Gen. "Chuck" Horner, USAF, in which Horner, who had been largely responsible for orchestrating the massive and brilliant air campaign, complained about the lack of current aerial photographs of exactly what his pilots were supposed to hit.[17] In testimony still on June 12, 1991, to the House Armed Services Committee (HASC), chaired by Congressman Les Aspin (Dem.-Wis.), General Schwarzkopf said:

> my major concern as a theater commander was the fact that the analysis had estimates that were coming out of consolidated analysis, and by the time we received them, they had been caveated, disagreed with, footnoted and watered down to the point that the estimate could have supported any outcome. When you were all done, no matter what the outcome was, they could say, "You see we were right in our estimate." That is not helpful to a commander in the field.[18]

Among other C^4ISR issues identified in Desert Shield/Desert Storm were the dissemination of the Air Tasking Order (ATO),[19] imagery dissemination,[20] and the need to improve Defense

---

[15]Ibid., Appendix K, K-47.

[16]U.S. Senate, *Operation Desert Shield/Desert Storm*, Hearings Before the Committee on Armed Services, 102nd Cong., 1st Sess., April 14; May 8, 9, 16, 21; June 4, 12, 20, 1991 (Washington, D.C.: U.S. Gov't Printing Office, 1991), 320.

[17]Ibid.

[18]U.S. House of Representatives, *The Impact of the Persian Gulf War and the Decline of the Soviet Union on How the United States Does Its Defense Business*, Hearings Before the Committee on Armed Services, 102nd Cong., 1st Sess., Feb. 27, March 4, 8, 12, 19, April 12, 16, 22, 25, 26, 30, May 1 and June 12, 1991 (Washington, D.C.: U.S. Gov't Printing Office, 1991), 930.

[19]For a detailed discussion of the difficulties involved in distributing the thousand-page Air Tasking Order (ATO), which contained the daily attack requirements for all coalition aircraft, see Allard, *Command, Control, and the Common Defense*, rev. ed., 284.

[20]For a brief, insightful explanation of the problems associated with imagery dissemination, see Arnold E. Donahue, "Perspectives on U.S. Intelligence," in *Seminar on Command, Control, Communications, and Intelligence,*

Support Program sensors,[21] but the point here is not to add to the literature on Desert Shield/ Desert Storm but, rather, to illustrate the difficulty for a commander in attempting to assess the factors associated with C^{4}ISR systems to determine whether information superiority over an adversary has been achieved.

Although there is little doubt that air and maritime superiority were achieved, did U.S. and coalition forces achieve information superiority over Iraqi forces during Operation Desert Shield/Desert Storm? Would anyone take a stand on this question, given the examples cited by General Schwarzkopf, that is, the inability of C^{4}ISR systems to pinpoint and destroy Scud missiles and other shortcomings of the C^{4}ISR systems that surfaced in the Pentagon's Final Report to Congress?

Chances are, a direct answer to these questions, if posed, might have been avoided. Officials would probably have been more comfortable describing U.S. C^{4}ISR systems as superior to Iraqi systems than claiming that the use of those systems resulted in (the condition of) information superiority. One example of the tendency to avoid directly answering such questions can be found in a statement attributed to General Schwarzkopf, who, despite his own criticisms expressed in the Capitol Hill hearings, declared:

> Our superiority in precision munitions, stealth, mobility, and command, control, communications and computers proved to be decisive force multipliers.[22]

5.3 Determining Information Superiority

The examples from Grenada and the Persian Gulf illustrate the difficulty of determining whether information superiority has or has not been achieved. If achieving information superiority becomes a declared objective of future military operations, commanders will need tools to aid them in making such determinations. One such tool might be an automated system capable of monitoring one's own C^{4}ISR infrastructure while probing an adversary's capabilities. For the scale shown in **Figure 4-1** to be useful, criteria need to be developed for determining the requisite information domain condition. Although this task appears difficult, and although no one has ever tried to develop such criteria before, it is probably possible. It would require technical work related to C^{4}ISR systems that would pose interesting engineering challenges, and the criteria would need to be an integral part of the overall command and control system. This system could display the condition on a computer in real time, as a system icon on the task bar, much as most Mac or Windows-based systems show the time and even date. Such a system would need to be

---

Guest Presentations, Spring 1997 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-98-2, April 1998), 109-110.

[21]See *Conduct of the Persian Gulf War*, Appendix K, K-49.

[22]Ibid., K-1.

able to detect intrusions, disruptions, and attacks while also providing commanders with options to counter them. Other features could include a capability that would assess an adversary's ability to use its own infrastructure. Offensive intrusion capabilities, along with tools to manipulate the adversary's perceptions might be useful to commanders, especially in face of a technologically sophisticated adversary.

Chapter Six

From Vision to Reality: Achieving an Integrated C4ISR Capability Without Another Goldwater–Nichols Act

> *Information Superiority combines the capabilities of intelligence, surveillance, and reconnaissance along with command, control, communications, computers, and intelligence to acquire and assimilate information needed to dominate and neutralize adversary forces and effectively employ friendly forces. Includes the capability for near-real-time awareness of the location and activity of friendly, adversary, and neutral forces throughout the battlefield area. Also includes a seamless, robust C4 network linking all friendly forces to provide common awareness of the current situation throughout the battlefield area.*[1]

Information superiority regarded as a condition is similar to air and maritime superiority, and the United States's current and future C4ISR capability is expected to provide the basis for achieving this condition. The C4ISR systems U.S. (and allied) forces use against an adversary are central to achieving information superiority during military operations. This report suggests the need for protected, integrated, and interoperable C4ISR systems to achieve information superiority over an adversary, and this chapter explores two possible scenarios in an effort to identify opportunities to improve the DOD's approach to C4ISR modernization and its enhancement of interoperability in support of future warfare concepts.

6.1 Information Superiority as an Objective of Joint Warfighting Capability

In 1996, the Joint Staff articulated twelve objectives of joint warfighting capabilities to "help provide a joint warfighting focus to a significant portion of the Defense Science and Technology program."[2] Information superiority was one of the objectives approved by the Joint Requirements Oversight Council (JROC).

A comparison of information superiority as part of General Shalikashvili's vision and as a JROC objective reveals that the JROC dropped the offensive portion of the capability desired in the *Joint Vision 2010*.[3] *Joint Vision 2010* sought a capability that would not only "collect, process, and disseminate an uninterrupted flow of information" but also "exploit or deny an adversary's ability to do the same." Development of this capability to exploit or deny an adversary's use of or trust in its information infrastructure was important to General

---

[1]Dept. of Defense, "The National Science and Technology Strategy," "Science and Technology Contributions to Military Capabilities," in *Defense Science and Technology Strategy* (Washington, D.C.: The Pentagon, May 1996; reprt. January 1997), 8.

[2]Ibid.

[3]Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: The Pentagon [1996]), 16.

Shalikashvili's vision, because it could be used, for example, to disrupt an adversary's information infrastructure, rendering it incapable of transmitting orders to control the course of an operation, or, if electronic, used to deceive or to manipulate perception. No official explanation for the omission from the JROC objective is available (but the offensive portion of the objective may have been dropped for security reasons).

6.2 Opportunities for Improving C^{4}ISR Modernization

Including offensive capabilities, regardless of application, in future C^{4}ISR systems to prevent an adversary from attaining information parity with U.S. forces would seem prudent. Given that future C^{4}ISR systems are expected to achieve information superiority,[4] as opposed to providing only information, requirements for future systems could be written to include both offensive and defensive features. The one joint warfighting capabilities objective (see the epigraph) that concerns achieving information superiority neither calls for integrated C^4 and ISR systems nor signals any intent to mandate joint requirements for C^{4}ISR systems. Thus, the problems remain of how expectations regarding C^{4}ISR systems are to be met and of how to improve the process for modernizing C^{4}ISR systems to ensure that future systems will be able to achieve information superiority.

The response that the services (and agencies) in the DOD ought to develop C^{4}ISR systems that satisfy the needs of the individual service or agency and then figure out how to make them compatible and interoperable after fielding in order to achieve information superiority seems unreasonable. The challenges of this approach—an approach used in the past—which are well documented[5] and have plagued the DOD, are often debated inside the Pentagon. For example, it is not unusual in the Pentagon to witness discussions or hear presentations about C^{4}ISR systems that claim that service-specific acquisition fosters a stovepipe approach[6] and that generally conclude by suggesting that this approach needs reform if C^{4}ISR systems are to be conceived jointly.[7] The effort in 1994 of the JROC, under the leadership of Admiral Owens, to find an innovative way to deal with this problem of stovepipe systems led to the emergence of a "system of systems" (see

---

[4]Because the nature of future conflicts will be either symmetric or asymmetric, an aim of this report is to provoke the reader into considering incorporating into future C^{4}ISR systems both defensive and offensive capabilities, such as capabilities for detecting electronic intrusion or for delivering virus or logic bombs.

[5]For a 1998 assessment and for findings related to issues of C^4 interoperability, see Office of the Director for C^4 Systems, The Joint Staff, *Warfighter Communications Study* (Washington, D.C.: The Pentagon, Feb. 23, 1998), 8-1—8-5.

[6]The stovepipe approach often results in dedicated or proprietary C^{4}ISR systems that operate independently of other systems. Stovepipe systems usually have unique, nonstandard characteristics.

[7]See, for example, charts from Capt. Tom Lang, USN, "Joint C^{4}ISR Battle Center," JBC Brief to C^{2}JWCA, slide presentation, Washington, D.C., The Pentagon, May 6, 1998, slide 2, [On-line]. URL: <http://www.jbc.js.mil/public/docs/index.html> (Accessed June 9, 1998.)

section **3.2**). The term C^4ISR was coined to represent a new way of looking at the disciplines of C^4, intelligence, surveillance, and reconnaissance. According to Admiral Owens:

> My feeling was that these disciplines which had themselves resided in stovepipes over the decades were inextricably ONE ENTITY. That what we were looking for was Real Time support for/and to the warrior, support that was much more than pictures of something which had happened or recounts of sigint (Signal Intelligence) events of the past but WHAT WAS HAPPENING NOW in the battlefield, even to the extent of being able to use the information to shoot a weapon at a target never seen by intrinsic sensors (a big step for any military). This was it seemed the key to effective optimal sensor to shooter development.[8]

A study directed by the JROC Review Board (JRB)[9] and conducted by the Command and Control Joint Warfighting Capability Assessment (C^2JWCA) team[10] and published in 1998 showed recent results of this stovepipe approach. The study identified many present or impending C^4 mismatches among the services and found C^4 problem areas between U. S. forces and allies or potential coalition partners. It specifically identified and summarized eighty-eight deficiencies related to C^4 interoperability alone.[11] Another report of 1998 highly critical of the DOD, the GAO report already mentioned[12] (see section **2.4**), found not only that the DOD processes for certifying the interoperability of existing, newly developed, and modified C^4ISR systems were ineffective but also that the policies were largely ignored by CINCs, services, and DOD agencies.[13]

There is skepticism that, in the face of declining budgets, the kind of change required to capitalize on information-age innovations will not take place unless it were to be legislated by Congress. Admiral Owens, for example, suggested to the Senate Armed Services Committee that "now [1998] is [the] time to consider a Goldwater–Nichols II,"[14] and he even outlined specific

---

[8]Personal communication by Admiral Owens to Anthony G. Oettinger, Nov. 12, 1998.

[9]The JROC Review Board (JRB) comprises flag officers from each service, designated by the JROC member of the particular service, and it is chaired by the JROC Secretary. Given that the JROC supports the Chairman of the Joint Chiefs of Staff in carrying out responsibilities, the JRB functions to assist the JROC.

[10]The Command and Control Joint Warfighting Capability Assessment (C^2JWCA) team consists of action officers from the services and defense agencies involved in the C^2 domain. The focus of the team is on providing connectivity to joint warfighters within a seamless, standardized environment and includes worldwide coverage and connectivity, which offers a fused-warrior domain as well as nuclear C^3I and sensor-to-shooter links.

[11]*Warfighter Communications Study*, 7-11—7-15.

[12]*Joint Military Operations: Weaknesses in DOD's Process for Certifying C^4I Systems' Interoperability*.

[13]Ibid., 4.

[14]Congressional testimony by Adm. William A. Owens, U.S. Senate, Committee on Armed Services, *National Defense Panel Hearings Before the Committee on Armed Services*, S. Hrg. 105-726, 105th Cong., 2nd Sess., Jan. 28-29, 1998 (Washington, D.C.: U.S. Gov't Printing Office, 1998), 44.

aspects of such legislation.[15] This suggestion carries weight, because many in Congress still regard the views of this former Chairman of the JROC as thoughtful, visionary, and provocative.[16] Even were Congress to have a sympathetic ear, however, drafting and implementing legislation such as Admiral Owens suggested would take a long time and, by his own admission, "a lot of blood will flow."[17]

Yet it may be possible to improve the modernization process for C^4ISR systems without the blood-letting of another Goldwater–Nichols Act. The following two scenarios explore some possibilities. Before exploring the first, however, some explanation of the DOD's JROC and the DOD's acquisition process is needed.[18]

6.2.1 The Joint Requirements Oversight Council (JROC)

Because, outside the Pentagon, little may be known about the JROC or its workings, a brief explanation may be helpful, although a comprehensive account of the JROC's procedures and policies regarding requirements lies beyond the scope of this report.[19]

In general terms, the JROC is made up of the vice-chiefs of each of the four services[20] and nominally chaired by the Chairman of the Joint Chiefs of Staff (CJCS), who routinely delegates

---

[15]Ibid. In his testimony, Adm. Owens suggested three essential parts of a Goldwater–Nichols II: (1) "that all military 'requirements' be determined by a 'JOINT' high-level civilian military group perhaps building on the JROC concept but with an Undersecretary or Deputy Secretary directly involved, properly supported with analysis and assessment capabilities, and that the services per se be taken out of the requirements process"; (2) "that the services be made clearly responsible for their infrastructure—the manning, training, and equipping of their troops, running their huge facility base like a CEO [chief executive officer] runs [a] company"; and (3) that each of what Adm. Owens called the "great enablers—Logistics, intelligence, Medical, and C3"—would be consolidated (as an executive agency, under one of the four services).

[16]Ibid., 38, 49.

[17]Ibid., 42.

[18]For more detailed information about the DOD's C^3I acquisition process, see Thomas P. Quinn, "Acquiring C^3I Systems for the Department of Defense: Process and Problems," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1994* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-95-3, January 1995), 1-28.

[19]For a comprehensive and detailed explanation of JROC procedures and policies, see the Office of the Chairman of the Joint Chiefs of Staff, *Charter of the Joint Requirements Oversight Council*, Instruction 5123.0 (Washington, D.C.: The Pentagon, May 2, 1997), [On-line.] URL: <http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/5123_01.pdf> (Accessed May 4, 1998.)]; and the Office of the Chairman of the Joint Chiefs of Staff, *Requirements Generations System*, Instruction 3170.01 (Washington, D.C.: The Pentagon, June 13, 1997), [On-line.] URL: <http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3170_01.pdf> (Accessed May 4, 1998.)

[20]Although in the past the members of the JROC have been the vice-chiefs of the services, the *Charter of the Joint Requirements Oversight Council*, provides the Chairman of the Joint Chiefs of Staff with some flexibility regarding JROC membership by stipulating that "members of the JROC will be selected by the Chairman of the Joint Chiefs of Staff, after consultation with the Secretary of Defense, from officers in the grade of general or admiral who are recommended for selection by the Secretary of their respective military department concerned" (Chairman of the Joint Chiefs of Staff, *Charter of the Joint Requirements Oversight Council*, Instruction 5123.01, Enclosure A, A-2).

the functions of the JROC chairmanship to the Vice Chairman of the Joint Chiefs of Staff.[21] The JROC assists the CJCS in identifying and assessing joint military requirements, including existing systems and equipment. The Council reviews warfighting requirements that may require new major defense acquisition programs[22] and makes judgments as to the consequences of solving particular deficiencies on the overall warfighting capability of U.S. forces. The JROC ordinarily limits its deliberations to issues associated with the most costly requirements and acquisition programs, which are known as Acquisition Category I (ACAT I)[23] programs.

6.2.2 Acquisition Categories

Validation (review of documentation by an operational authority other than the user to confirm a need or operational requirement) and approval (formal or official sanction of the need identified, as described in the requirements documentation) authority in the DOD's requirements generation system are ordinarily based on dollar threshold levels associated with the DOD's acquisition categories (dollar thresholds for which are expressed in fiscal year 1996 constant dollars).[24] There are four categories:

1. **Acquisition Category I (ACAT I)** programs are major defense acquisition programs designated by the Under Secretary of Defense (Acquisition and Technology) (USD[A&T])[25] as such or estimated to require an eventual total expenditure of more than $355 million for research, development, test, and evaluation or more than $2.135 billion for procurement.

2. **Acquisition Category IA (ACAT IA)** programs are major automated information system programs designated by the ASD(C^3I)[26] as such or estimated to require program costs in any single year in excess of $30 million, total program costs in excess of $120 million, or total life cycle costs in excess of $360 million.

---

[21]Ibid.

[22]Major defense acquisition programs are defined in 10 U.S. Code; Armed Forces; Subtitle A—General Military Law, Sec. 2430, Major Defense Acquisition Programs.

[23]For a complete list of 1997 Major Defense Acquisition Programs, which lists approximately twenty ACAT I C^4ISR programs in the DOD, see [On-line] at URL: <http://www.acq.osd.mil/api/asm/mdaplist.html> (Accessed May 1, 1998.)

[24]For detailed information regarding the DOD's acquisition categories, see *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*, DOD Regulation 5000.2-R, Change 3, Part 1, "Acquisition Management Process" (Washington, D.C.: The Pentagon, March 23, 1998), 1-4.

[25]The Under Secretary of Defense (Acquisition and Technology) (USD[A&T]) is the senior procurement executive for the DOD and, as such, establishes policies for acquisition (including procurement, research and development, logistics, developmental testing, and contract administration) for all elements of the DOD.

[26]The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C^3I]) has as the principal duty the overall supervision of command, control, communications, and intelligence affairs of the DOD.

3. **Acquisition Category II (ACAT II)** programs do not meet the criteria for an ACAT I program but do meet the criteria for a major system.[27] ACAT II programs usually are estimated to require an eventual total expenditure for research, development, test, and evaluation of more than $135 million or for procurement more than $640 million.

4. **Acquisition Category III (ACAT III)** programs do not meet the criteria for an ACAT I, ACAT IA, or an ACAT II program. This category also includes less-than-major automated information system programs.

6.2.3 Management of Defense Acquisition Programs

One effect of categorizing defense acquisition programs is to ease overall management by separating major programs from lesser ones, for which the USD(A&T) may delegate responsibility for oversight. The major defense acquisition programs, because of their high dollar thresholds, come under the direct supervision of the USD (A&T), while lesser programs are usually delegated to a Component Acquisition Executive (CAE). The major programs are closely scrutinized by congressional committees, and the DOD emphasizes their management. For example, for ACAT I programs, the JROC supports the DOD's Defense Acquisition Board (DAB)[28] process by reviewing costs, objectives, schedule, and key performance parameters (capabilities or characteristics considered essential for successful mission accomplishment) prior to milestone (major decision points that separate the phases of an acquisition program)[29] decision reviews (for a diagram of the acquisition phases and milestones for orderly translation of broadly stated mission needs into system-specific performance requirements, see **Figure 6-1**).[30]

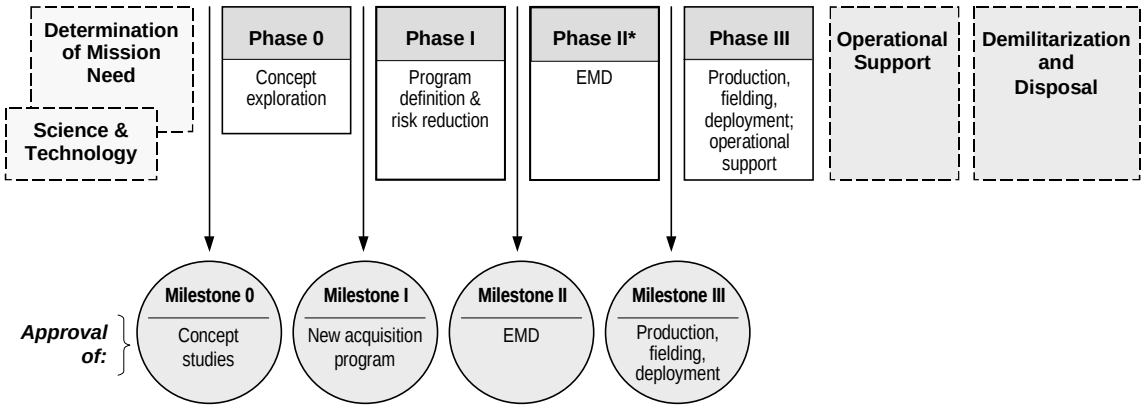
---

[27]Major systems are defined in 10 U.S. Code; Armed Forces; Subtitle A—General Military Law, Sec. 2302(5), Definitions.

[28]The Defense Acquisition Board is the senior advisory body to the USD(A&T), advising the USD(A&T) on policies and procedures governing the operations of the DOD acquisition system. The USD(A&T) chairs and the VCJCS vice-chairs the DAB, pursuant to Dept. of Defense, *Defense Acquisition*, Directive 5000.1 (Washington, D.C.: The Pentagon, March 15, 1996), 12. The schedule of the DAB is available [On-line] at URL: <http://www.acq.osd.mil/api/asm/dabschdl.html> (Accessed May 1, 1998.)

[29]Dept. of Defense Acquisition Deskbook, CD-ROM version 2.6, section 2.3, Acquisition Process (Wright-Patterson AFB, Ohio, December 1998).

[30]Dept. of Defense, Defense Acquisition Deskbook, CD-ROM version 2.1, section 2.3, Acquisition Process (Wright-Patterson AFB, Ohio, Sept. 30, 1997).



EMD = engineering, manufacturing, and development
*May include low-rate initial production (LRIP).
Source: Adapted from Defense Acquisition Deskbook, CD-ROM version 2.6, December 1998.

Figure 6-1

Defense Acquisition Phases and Milestones

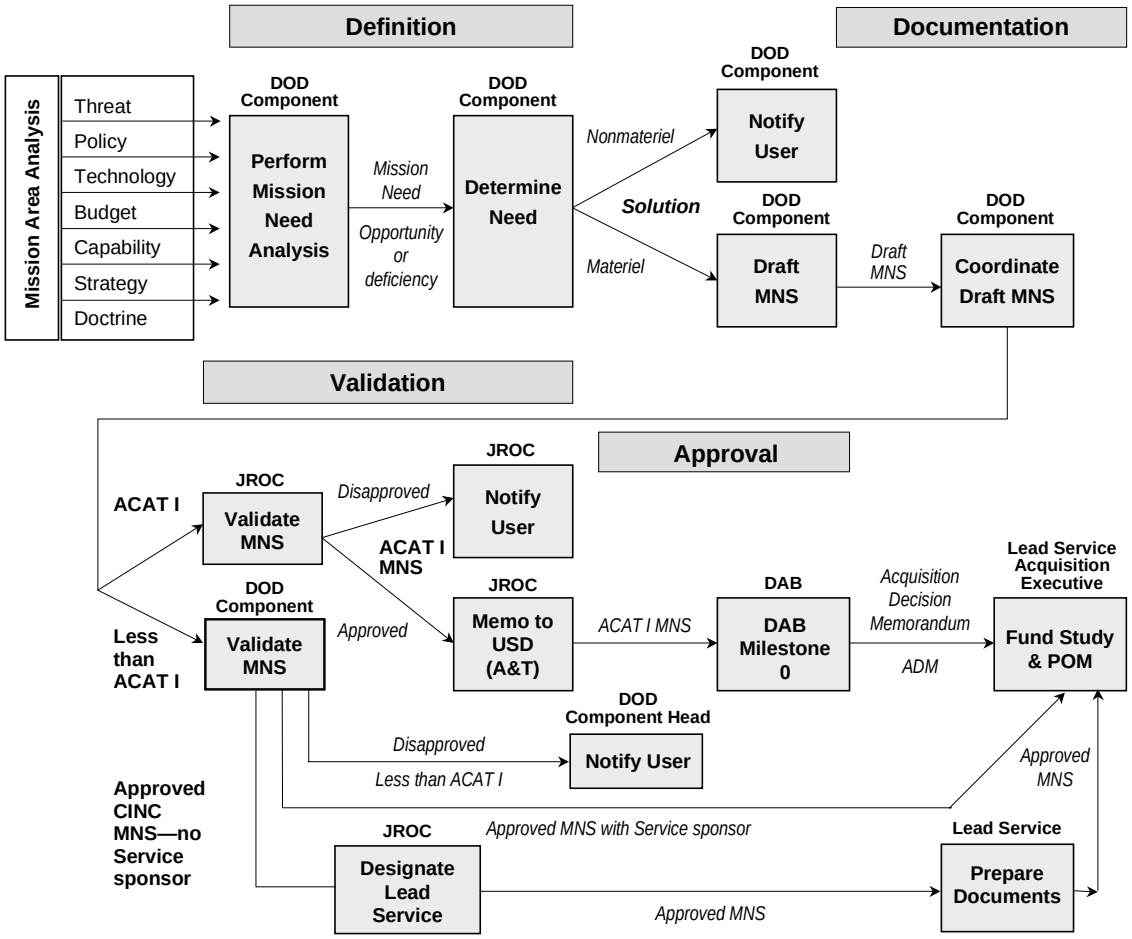
6.2.4 Operational Requirements

The Chairman of the Joint Chiefs of Staff provides advice and recommendations on operational requirements to the Secretary of Defense.[31] The Chairman evaluates and integrates requirements to promote efficiency and avoid unnecessary duplication. Using the JROC as a means to accomplish these functions, all potential ACAT I mission need statements (MNSs)[32] and all ACAT I operational requirements documents (ORDs)[33] are validated and approved by this Council. **Figure 6-2** indicates the substance of the system and depicts how MNSs are generated. Creation of ORDs follows a similar pattern. The JROC also assesses the expected level of joint DOD component involvement before the approved mission need (a deficiency in current capabilities or an opportunity to provide new capabilities through the use of new technologies) is submitted to the USD(A&T). When these military requirements enter the realm of the Office of the Secretary of Defense (OSD), they also enter the DAB process. The process is highly visible, and DAB programs are ordinarily subject to stringent oversight by DOD officials and members of Congress. The JROC generally remains involved in ACAT I programs throughout the full

[31]This authority is set forth in detail in 10 U.S. Code; Armed Forces; Subtitle A—General Military Law, Sec. 153, Chairman: functions and 163, Role of the Chairman of the Joint Chiefs of Staff.

[32]A mission need statement is a formatted statement not specific to a particular system that presents operational capability needs in broad operational terms.

[33]An operational requirements document is a formatted statement containing performance and related operational parameters for a proposed concept or system. ORDs are prepared by the user or user's representative at each milestone, beginning with Milestone I.



ACAT = Acquisition Category
CINC = commander in chief
JROC = Joint Requirements Oversight Council
DAB = Defense Acquisition Board
DOD = Department of Defense
MNS = mission need statement
POM = program objective memorandum
USD (A&T) = Under Secretary of Defense (Acquisition and Technology)

Source: Chairman of the Joint Chiefs of Staff, *Requirements Generation System,* Instruction 3170.01 (Washington, D.C.: The Pentagon, June 13, 1997), Enclosure A, A-2.

Figure 6-2

Mission Need Statement Generation Process

development cycle of a program, reviewing costs, objectives, schedule, and, in particular, key performance parameters, to ensure that mission needs are satisfied prior to all DAB major milestone decision reviews.

6.3 Scenario 1: Increased Use of Executive Committees

The first scenario is intended to suggest that the responsibility for validation and approval of C^4ISR ACAT II and ACAT III MNSs and ORDs could be assigned to a joint military committee, and, further, that such a committee could review joint potential, costs, objectives,

schedule, and key performance parameters for designated C4ISR ACAT II and III programs before every major milestone decision.

The current (1999) JROC and DAB process works well, but only for ACAT I programs. What it does not address is that many C4ISR programs fall into the ACAT II and most into the ACAT III category. The number of C4ISR ACAT II and III programs far exceeds that of ACAT I programs in the DOD,[34] leaving little opportunity for cross-service integration of requirements in an area that might thrive on integration. Most ACAT II and almost all ACAT III mission needs are submitted by a service,[35] then validated and approved by a service chief or designated representative of the same service. After approval, the mission needs are turned over to the service acquisition executive, who implements programs, using service program executive officers and service program or product managers. This practice, if not modified, will continue to result in little integration of the thousands[36] of networks and communications devices that make up the DOD's C4ISR systems[37] infrastructure. To the extent that the DOD wants protected, integrated, and interoperable C4ISR systems capable of achieving its stated goal of information superiority, expansion of joint executive committees may be one way to achieve it.

A new executive committee[38] could be established or the charter of an existing committee expanded at the Lieutenant General/Vice Admiral level, with responsibility for validation and approval of C4ISR ACAT II and ACAT III MNSs and ORDs delegated to the committee's chairperson. The makeup and functions of this committee could be modeled on the JROC,[39] with an advisory function added for ACAT I programs. The component acquisition oversight and review structure would remain responsible for acquisition matters of phase II and beyond (see

---

[34]A complete list of 1997 Major Defense Acquisition Programs indicates approximately twenty ACAT I C4ISR programs in the DOD [On-line]. URL: <http://www.acq.osd.mil/api/asm/mdaplist.html> (Accessed May 1, 1998.)

[35]Submission of an MNS is not limited to the services. As indicated in Figure 6-2, all DOD components—OSD, the Military Departments, the Chairman of the Joint Chiefs of Staff (Joint Staff), the unified and specified commands (including U.S. element, North American Aerospace Defense [NORAD] Command, defense agencies, and DOD field activities—may submit MNSs.

[36]On Sept. 14, 1993, in an address to Federal Sources, Inc., in Vienna, Va., Emmett Paige, Assistant Secretary of Defense for C3I, indicated that there were (at least) 10,000 C2 systems in the DOD; cited in Kenneth Allard, *Command, Control, and the Common Defense*, rev. ed. (Washington, D.C.: NDU Press, INSS, October 1996), 292.

[37]U.S. GAO/NSIAD, *Joint Military Operations; Weaknesses in DOD's Process for Certifying C4I Systems' Interoperability* ([Washington, D.C.: GAO/NSIAD-98-73, March 1998], 4), states that, as of December 1997, the DOD Defense Integration Support Tool database of C4 systems listed about 1,000 systems that may exchange information with another system and added that there are also about 1,176 unclassified intelligence systems.

[38]To ensure that such a committee has appropriate authority, this committee might be added to Chapter 7 (Boards, Councils, and Committees) of Part I (Organization and General Military Powers) of 10 U.S. Code; Armed Forces; Subtitle A–General Military Law.

[39]The idea of using a joint, high-level group, building on the JROC concept, for all military requirements was introduced by Adm. Owens in congressional testimony, U.S. Senate, Committee on Armed Services, *National Defense Panel Hearings Before the Committee on Armed Services*, S. Hrg. 105-726, 105th Cong., 2nd Sess., Jan. 28-29, 1998 (Washington, D.C.: U.S. Gov't Printing Office, 1998).

Figure **6-1**), but, in addition to validation and approval of ACAT II and III MNSs, this new joint three-star level "Joint C4ISR Requirements Committee" would review ACAT II and III ORDs before major milestone decisions for joint potential, costs, objectives, schedule, and key performance parameters.

In the Pentagon, the creation of a new committee often meets something less than enthusiasm, so that expanding the charter of an already existing executive committee may be worth exploring. Among existing DOD committees, three, in one form or another, have both an interest and expertise in C4ISR programs, although no DOD committee (with the exception of the JROC; see section **6.2.1**) has authority to validate or approve C4ISR systems requirements. Authority for approval for ACAT I MNSs and ORDs lies with the JROC, but for ACAT II/III it has been delegated to service chiefs or their representatives.[40]

6.3.1 Existing DOD Executive Committees

The three existing executive committees with an interest and expertise in C4ISR systems are the Military Intelligence Board, the Military Communications-Electronics Board, and the DOD Chief Information Officer (CIO) Council. A comprehensive review of these committees and their charters would be necessary before any recommendations could be made of which was best suited to perform the new functions suggested. (The review, which is beyond the scope of this report, would require further study.) The following are brief, general descriptions of the three committees.

Military Intelligence Board (MIB). The MIB is chaired by the Director of the Defense Intelligence Agency (DIA), whose members consist mainly of the heads of the DOD intelligence components and others. The MIB serves as a forum for discussion of intelligence requirements and support and as an advisory body to assist the Director of DIA. It has no executive authority and its recommendations and actions are not intended to alter the missions, responsibilities, functions, authorities, and resources assigned to any DOD component.[41]

Military Communications-Electronics Board (MCEB). The MCEB is chaired by the Joint Staff's Director, C4 Systems, and its members primarily consist of the heads of DOD C4 systems components and others. It serves as a forum to consider C4 systems matters, and it

---

[40]For a detailed account, see Chairman of the Joint Chiefs of Staff, *Requirements Generation System*, Instruction 3170.01 (Washington, D.C.: The Pentagon, June 13, 1997), A-4, [On-line]. URL: <http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3170_01.pdf> (Accessed May 4, 1998.)

[41]For more information about the MIB, see Dept. of Defense, *Defense Intelligence Agency (DIA)*, Directive 5105.21 (Washington, D.C.: The Pentagon, Feb. 18, 1997).

coordinates DOD components and others.[42] The MCEB is responsible for the enforcement of policy regarding compatibility, interoperability, and integration of C^4I systems.[43]

DOD Chief Information Officer (CIO) Council. This council, chaired by the Department's Chief Information Officer, who is the Pentagon's top C^3I official, was established as a direct result of the Information Technology Management Reform Act (ITMRA) of 1996 and a subsequent Secretary of Defense Memorandum.[44] It is made up of the chief information officers of the services and selected other DOD officials, with the director of the Defense Information Systems Agency serving as technical advisor.[45] The council is the principal DOD forum advising the Secretary and Deputy Secretary of Defense on the full range of matters pertaining to information technology; exchanging pertinent information and discussing issues related to DOD information technology and information technology management. It is responsible for coordinating implementation of activities under subdivision E of the Clinger–Cohen Act of 1996 (Public Law 104-106) in DOD.[46]

6.3.2 Advantages and Disadvantages of Executive Committees

The advantages of using a joint executive committee to validate and approve ACAT II/III C^4ISR requirements is that such a committee could assist in the enforcement of DOD policy, which states "that, for purposes of compatibility, interoperability, and integration, all C^3I systems developed for use by U. S. forces are considered to be for joint use."[47] It would seem prudent for the DOD to capitalize on the wisdom and experience of military executives with a background of C^4ISR operational assignments to share the responsibility for modernizing C^4ISR systems, improving their interoperability. The committee could, for example, guard against having a process in which the mission needs or opportunities of one service, seeking its future capability, were introduced without consideration for the potential needs of another service. Another advantage is that it could be used to accelerate, synchronize, expand, combine, separate, or realign all C^4ISR programs, as necessary, and even eliminate obsolete and duplicative systems.

There would also be disadvantages in using a joint executive committee to validate and approve ACAT II/III C^4ISR requirements and review such programs prior to major milestone

---

[42]For more information about the MCEB, see Dept. of Defense, *Military Communications–Electronics Board*, Directive 5100.35 (Washington, D.C.: The Pentagon, March 10, 1998).

[43]Chairman of the Joint Chiefs of Staff, *Compatibility, Interoperability, and Integration of C^4I Systems*, Instruction 6212.01A (Washington, D.C.: The Pentagon, June 30, 1995).

[44]Dept. of Defense, *Implementation of Subdivision E of the Clinger–Cohen Act of 1996 (Public Law 104-106)*, Memorandum with Attachments (Washington, D.C.: The Pentagon, June 2, 1997).

[45]Ibid., with Attachment 2, *Charter, Department of Defense Chief Information Officer Council*.

[46]Ibid.

[47]Dept. of Defense, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C^3I) Systems*, Directive 4630.5 (Washington, D.C.: The Pentagon, Nov. 12, 1992), 2.

decisions for joint potential, costs, objectives, schedule, and key performance parameters. One considerable disadvantage would be possibly adding to an already lengthy C4ISR modernization process. Reviewing all existing and potential C4ISR programs at all ACAT levels[48] represents a significant workload, either for the new joint C4ISR Requirements Committee or for one of the three committees discussed in section **6.3.1**. A second disadvantage might be that issues that require committee consensus might be compromised to the point where resolution would be achieved at the lowest common denominator just to get on with the particular program. An issue that might be perceived as a further disadvantage is that the services now have authority to validate and approve most ACAT II/III MNSs and ORDs and therefore have in place a structure that supports that process. Were authority for validation and approval for ACAT II/III C4ISR MNSs and ORDs given to a joint committee while for all other ACAT II/III programs the status quo obtained, an added support structure for this committee would be needed. Finally, taking validation and approval authority away from the services and giving it to the chairperson of a joint executive committee might meet significant resistance from the services. Even if such authority were established by law, funding validated and approved C4ISR programs is far from automatic and is subject to internal processes of the services,[49] which could elect to fund these programs selectively.

6.4 Scenario 2: C4ISR Concept Exploration and Demonstration

The second scenario involves only the first two phases of the acquisition process, namely, Phase 0, Concept Exploration, and Phase I, Program Definition and Risk Reduction (see **Figure 6-1**). Like Scenario 1, this scenario is illustrated within the existing DOD requirements and acquisition framework.

6.4.1 Phase 0, Concept Exploration

Phase 0 typically consists of short-term concept studies to define and evaluate the feasibility of alternative concepts and to provide a basis for assessing their relative merits (i.e., advantages and disadvantages, degrees of risk). Analysis of alternatives is used to compare different concepts. As a result of these studies, the most promising system concepts are defined in terms of broad objectives for cost, schedule, performance, software requirements, opportunities for tradeoffs, overall acquisition strategy, and test and evaluation strategies.[50]

---

[48]An assumption is made that, given the option, the JROC would seek the advice of this committee on ACAT I C4ISR issues.

[49]For an example of a requirement validated and approved by the JROC but not funded by the service responsible for the program, see Quinn, “Acquiring C3I Systems for the Department of Defense: Process and Problems,” 8.

[50]Defense Acquisition Deskbook, CD-ROM version 2.6, Section 2.3, Acquisition Process, Phase 0, Concept Exploration.

6.4.2 Phase I, Program Definition

During Phase I, programs are defined while one or more concepts, design approaches, or parallel technologies are pursued. Assessments of advantages and disadvantages of alternative concepts are defined. Prototyping, demonstrations, and early operational assessments are considered and performed, as necessary. Cost drivers, life-cycle cost estimates, cost-performance trades, interoperability, and acquisition strategy alternatives are considered.[51]

6.5 Joint C^{4}ISR Concept Exploration and Demonstration Center

Scenario 2 suggests that responsibility for Phases 0 and I for all C^{4}ISR programs could be assigned to a Joint C^{4}ISR Concept Exploration and Demonstration Center.

Were all the comments, criticisms, and counsel over the years from countless well-meaning defense analysts, C^{4}ISR professionals, and others concerning the DOD's C^{4}ISR systems looked at together (see section **2.4**), they might reveal as a common thread the view that the DOD's C^{4}ISR requirements and its modernization process have been optimized to take care of the needs of a particular service, as opposed to the needs of the joint force commander. Regardless of whether such commentary is right or wrong, the current process indisputably causes interoperability problems, as the GAO and others have pointed out (see section **6.2**). In the end, such problems come with the territory—that is, fielding a high-technology, mobile, agile, and lethal force. Yet the criticisms merit consideration, given that the vision of the future is based on a smaller, more lethal, multidimensional force that is expected to carry out synchronized military operations relying on protected, integrated, and interoperable C^{4}ISR systems.

It seems simple enough to examine current C^{4}ISR requirements and the process of modernization in order to identify opportunities for requirements integration or to see whether any exist. The question becomes, does the DOD have a process that encourages development of integrated C^{4}ISR systems or of systems at least designed to work together as part of an overall C^{4}ISR network? According to the first scenario (see section **6.3** and the subsections within it), authority for validation and approval for most C^{4}ISR needs rests with the services, because many of those needs do not reach the ACAT I thresholds. Thus, opportunities for change there are limited. Once a need has been validated and approved, a project moves on for short-term concept studies and program definition. In most cases, these efforts are conducted within a single service. Again, opportunities for integration are limited; but there are occasional exceptions. Depending on the complexity of a project, a joint program office may be established or liaison teams used to conduct the work of Phases 0 and I. In these cases, therefore, though more the exception than the rule, opportunities for requirements integration present themselves on an ad hoc basis.

---

[51]Ibid., Phase 1, Program Definition and Risk Reduction.

If the DOD wants integrated C4ISR systems, this approach might be taken a step further for C4ISR systems, even without a Goldwater–Nichols II. Specifically, the DOD could establish a permanent Joint C4ISR Concept Exploration and Demonstration Center, with the mission of taking all approved C4ISR MNSs from the JROC and other validation and approval authorities, conducting concept exploration and program definition work, and, after the Center had gained milestone II approval,[52] handing the program over to a service for the remaining phases of the acquisition process, e.g., engineering, manufacturing, and development (EMD), and so on for the remaining phases (see **Figure 6-1**).

A Joint C4ISR Concept Exploration and Demonstration Center could provide a place from which to view and assess the baseline C4ISR network. It could be set up as a C4ISR "center of excellence" solely for the purpose of C4ISR concept exploration and demonstration, to be staffed by all the services and equipped with state-of-the-art simulation technology.[53] It could, for example, examine how the C4ISR network would react to changes and evaluate how to optimize the network. More important, it could identify where a more efficient flow of information between network components and among various weapons could provide the joint force commander with additional options when faced with many targets. It could, simply, offer a better understanding of the overall capability as it now exists, explore potential solutions to possible future problems based on that understanding, and visually display logical options for new opportunities and improvements to help decisionmakers.

6.5.1 Existing Joint Organizations

The creation of any new DOD overhead organization, such as a Joint C4ISR Concept Exploration and Demonstration Center, like the creation of a new committee in the Pentagon, would meet something less than wild enthusiasm, which, here too, might make expanding the charter of an existing organization worth consideration. Several organizations now, in one form or another, have expertise in C4ISR concept exploration and demonstrations: (1) the Joint Warfighting Center, (2) the Joint C4ISR Battle Center, (3) the Joint C4ISR Decision Support Center, and (4) the Joint Interoperability Test Command. Certainly, these four are not all the joint organizations with both an interest and expertise in the area of C4ISR concept exploration and demonstration, but these would be a useful part of any analysis of existing joint organizations

[52]Milestone II approval allows a program to enter the engineering, manufacturing, and development phase of the acquisition process.

[53]The feasibility of this idea is supported by the emergence of simulation facilities such as the Reality Center in Orlando, Fla., which opened Nov. 5, 1997, and which enables battlefield visualization or mission rehearsal, cockpit instrumentation, dismounted or individual combatant capabilities, helmet-mounted technology, and firearms training. Private sector companies have embraced the concept of simulation facilities, for example, Texaco's recently established visualization centers which allow geologists, geophysicists, and petroleum engineers to view and manipulate different types of subsurface data simultaneously.

considered capable of potentially assuming the responsibility for Phases 0 and I for all C4ISR programs.

The following descriptions of these organizations are intended not to be comprehensive but to provide sufficient information to support the assertion here that each has both interest and expertise in the area of C4ISR concept exploration and demonstration:

1. **The Joint Warfighting Center (JWFC)**,[54] located at Fort Monroe, Hampton, Virginia, is a Joint Chiefs of Staff organization designed to enhance joint operations and training. Among other things, it facilitates the implementation of *Joint Vision 2010*.[55] It develops future operational and supporting concepts, assists in developing a strategy to evaluate alternative operational and organizational designs, materiel, systems, and concepts, and, in general, integrates efforts of the joint community.[56]

2. **The Joint C4ISR Battle Center**[57] was established in 1996 to provide an experimental environment for rapid, near-term insertion of C4ISR technology. It is located in Suffolk, Virginia, at the same site as the United States Atlantic Command's Joint Training, Analysis, and Simulation Center (JTASC). The Joint C4ISR Battle Center supports *Joint Vision 2010*[58] by ensuring that information superiority is achieved by enhancing the C2 process through technology innovations in the key enabling areas of C4ISR.

3. **The Joint C4ISR Decision Support Center**[59] was established in 1996 to provide quantitative and qualitative analysis on selected C4ISR issues in support of the DOD's senior requirements and acquisition decisionmakers. The Center, located in Crystal City, Virginia, brings together OSD, Joint Staff, service, CINC, Defense agency, and industry experts to identify integrated solutions to joint C4ISR issues.

4. **The Joint Interoperability Test Command (JITC)**[60] is responsible for conducting the DOD's C3I systems interoperability testing and certification program. It is located at Ft. Huachuca, Arizona, with a mission to bring C4I interoperability support, operational field assessments, and technical assistance to the CINCs, services, and Defense agencies.

---

[54]For more information on the Joint Warfighting Center, see the Center's Home Page, at URL: <http://www.jwfc.js.mil/> (Accessed May 29, 1998.)

[55]*Joint Vision 2010.*

[56]Joint Warfighting Center, Concepts Division, Mission, [On-line]. URL: <http://www.jwfc.js.mil/pages/Jvdiv.htm> (Accessed May 29, 1998.)

[57]For more information on the Joint C4ISR Battle Center, see the Center's Home Page, at URL: <http://www.jbc.js.mil> (Accessed March 6, 1998.)

[58]*Joint Vision 2010.*

[59]For more information on the joint C4ISR Decision Support Center, see the Center's Home Page, at URL: <http://134.152.187.26/dsc/index.htm> (Accessed May 22, 1998.)

[60]For more information on JITC, see the JITC Home Page, at URL: <http://www.jitc-emh.army.mil> (Accessed May 22, 1998.)

6.5.2 Advantages and Disadvantages of a Joint C4ISR Concept Exploration and Demonstration Center

There are considerable advantages to using a joint center for C4ISR concept exploration and demonstration for Phases 0 and I while leaving the military services for the remaining phases of the acquisition process. The Center could function as outlined in this scenario, without infringing on the powers of the services. It could conduct concept exploration and program definition work while leaving EMD, fielding, etc., of the systems to the services or to the appropriate Defense agencies, hence facilitating the development of protected, integrated, and interoperable C4ISR systems without infringing on the services' responsibility to organize, train, and equip. The Center could promote jointness, interoperability, and C4ISR systems integration during concept formulation, rather than attempting it as part of a bureaucratic approval process. Its establishment could revolutionize the current C4I requirements certification process, which requires that all MNSs and ORDs conform to joint C4/C4I policy and doctrine, architectural integrity, and interoperability standards.[61] And its establishment might also provide an opportunity to review all organizations that currently conduct C4ISR concept exploration and demonstration work, thereby potentially identifying offsets for the resources necessary to operate the Center.

There would also be disadvantages to separating Phases 0 and I from the remaining phases by dividing authority over the acquisition process between a new joint Center for the first two phases and the services[62] for the remaining ones. One disadvantage would be that the DOD already has a uniform requirements and acquisition process that functions well: all mission needs, requirements, and programs are processed in accordance with it, and they all follow the same path. Treating C4ISR programs differently might introduce confusion into a well-organized system; and it would add to the workload, because the Center would undoubtedly generate C4ISR-specific activity, which in most cases would require additional staff. A second disadvantage would be that the Center would itself need to be staffed with experienced C4ISR professionals already most likely contributing elsewhere within the DOD.

Another potential disadvantage would be that creating a Joint C4ISR Concept Exploration and Development Center might confuse well-established lines of authority among a program

---

[61]The requirements certification process requires a review of all MNSs and ORDs, regardless of acquisition category, for conformance to C4/C4I policy and doctrine, architectural integrity, and interoperability standards. The process is described in Chairman of the Joint Chiefs of Staff, *Compatibility, Interoperability, and Integration of C4I System*, Instruction 6212.01A (Washington, D.C.: The Pentagon, June 30, 1995), B-2. The criteria used to assess ORDs for requirements certification are available in the Defense Acquisition Deskbook, CD-ROM version 2.1, section 1.1.5.1, Defense Information Systems Agency (DISA) Assessment Criteria of ORD (Wright-Patterson AFB, Ohio, Sept. 30, 1997). Chairman of the Joint Chiefs of Staff, *Requirements Generation System*, Instruction 3170.01 ([Washington, D.C.: The Pentagon, June 13, 1997], A-5, A-6) assigns the Joint Staff's C4 Systems Directorate the responsibility to certify that all MNSs and ORDs conform to C4/C4I policy and doctrine, architectural integrity, and interoperability standards.

[62]Or defense agencies.

manager, program executive officer, and component acquisition executive. A further disadvantage would be the potential instability of a program. The services make serious efforts to stabilize programs, and moving a program from one location to another after obtaining Milestone II approval might introduce unnecessary turmoil.

6.6 Combining the Two Scenarios

Other scenarios undoubtedly exist, but these two seemed appropriate to the purpose here of suggesting how the DOD might improve its C^4ISR modernization approach and enhance interoperability in support of future warfare concepts. Implementing either of them would not provide a panacea, but if the goal is combat synchronization and if information superiority is the enabling condition, either would be useful. Although developed for separate consideration, were the two scenarios combined, the result might be a far more dynamic joint C^4ISR modernization approach and means to enhance interoperability than either alone offers.

Chapter Seven

Summary

Future military operations may not be limited to air (including space), land, and sea warfare but could include a new dimension—cyberspace. Information operations may become as commonplace as ground, maritime, or air operations were in the 1990–91 war in the Persian Gulf. The DOD will need therefore to supplement its overall military capabilities with information-age technologies—that is, it will need to develop and maintain protected, integrated, and interoperable C^4ISR systems that include both offensive and defensive capabilities. Just as maritime assets are used to achieve maritime superiority and air assets to achieve air superiority, so C^4ISR systems may be used to achieve information superiority against future adversaries.

Achieving information superiority means different things to different people. In 1996, *Joint Vision 2010*[1] first brought the term information superiority into the spotlight, portraying it as a *capability*: " a capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[2] According to the QDR completed in 1997, information superiority is an *ability*: "the ability to collect and distribute to U.S. forces throughout the battlefield an uninterrupted flow of information, while denying the enemy's ability to do the same."[3] This report suggests that information superiority is instead a *condition*: like air and maritime superiority, it is a condition that planners and warriors need to establish in order to gain an operational advantage and to minimize risks associated with an overall campaign. Achieving maritime, air, or information superiority is the condition that forms the basis for the successful conduct of future campaigns.[4]

Measuring information superiority in the midst of, or even after completion of, a military operation is difficult, but it is possible to assess the performance of C^4ISR systems in past military operations. Here, two military campaigns already judged successful are examined, the invasion of Grenada in 1983 and the war in the Persian Gulf in 1990–91, to illustrate the operational and political difficulties involved in any attempt to measure whether information superiority was

---

[1]Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: The Pentagon [1996]).

[2]Ibid., 16.

[3]William S. Cohen, Secretary of Defense, in "The Secretary's Message," in "What's New?" *Report of the Quadrennial Defense Review* (Washington, D.C.: The Pentagon, May 1997), [On-line]. URL: <http://www.defenselink.mil/pubs/qdr/msg.html> (Accessed July 20, 1998.)

[4]According to *Joint Warfare of the Armed Forces of the United States*, gaining air superiority and maritime superiority were preconditions for further operations during the 1990-91 Persian Gulf War. See *Joint Warfare of the Armed Forces of the United States*, 2nd ed. (Washington, D.C.: The Pentagon, Joint Publication 1, Jan.10, 1995), Appendix A, A-3, [On-line]. URL: <http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf> (Accessed March 12, 1998.)

achieved. A graduated, six-point scale of information domains (see **Figure 4-1**) posits a range of conditions from information inferiority to information supremacy.

For U.S. forces to achieve information superiority over an adversary, they must have protected, integrated, and interoperable C^4ISR systems designed for joint operations. To determine how the DOD could field such systems, some opportunities are explored to improve the DOD's approach to modernizing C^4ISR systems and to enhance interoperability. Two scenarios for the development of concepts and means to apply them are discussed, first, the establishment of a Joint C^4ISR Requirements Committee, and, second, the creation of a Joint C^4ISR Concept Exploration and Demonstration Center. Although these scenarios are offered separately, accepting both, or, better, combining them, would result in a more integrated approach to modernization of C^4ISR systems and enhancing interoperability in support of warfare in the information age.

Acronyms

ACAT	Acquisition Category
ACTD	Advanced Concept Technology Demonstration
AFCEA	Armed Forces Communications and Electronics Association
AI	artificial intelligence
AIMD	Accounting and Information Management Division (GAO)
ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ATO	Air Tasking Order
C^2	command and control
C^2JWCA	Command and Control Joint Warfighting Capability Assessment
C^3	command, control, and communications
C^3I	command, control, communications, and intelligence
C^4	command, control, communications, and computers
C^4I	command, control, communications, computers, and intelligence
C^4IFTW	command, control, communications, computers and intelligence for the warrior
C^4ISR	command, control, communications, computers and intelligence, surveillance, and reconnaissance
CAE	component acquisition executive
CD-ROM	compact disc–read only memory
CEO	chief executive officer
CINC	commander in chief
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CMA	C^4ISR Mission Analysis
DAB	Defense Acquisition Board
DEFCON	Defense Readiness Conditions
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
DRI	Defense Reform Initiative
EIA	Electronic Industries Association
EMD	engineering, manufacturing, and development
GAO	General Accounting Office
HAC	House Appropriations Committee
HASC	House Armed Services Committee

I	intelligence
INSS	Institute for National Strategic Studies
ISX	Information Superiority Experiment
IT	information technology
ITMRA	Information Technical Management Reform Act of 1996
JBC	Joint C^4ISR Battle Center
JITC	Joint Interoperability Test Command
JRB	JROC Review Board
JROC	Joint Requirements Oversight Council
JTASC	U.S. Atlantic's Joint Training, Analysis, and Simulation Center
JTR	Joint Tactical Radio
JWCA	Joint Warfighting Capability Assessment
JWFC	Joint Warfighting Center
JWID	Joint Warrior Interoperability Demonstration
LRIP	low-rate initial production
MAIS	Major Automated Information System
MCEB	Military Communications-Electronics Board
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MIB	Military Intelligence Board
MNS	mission need statement
NDP	National Defense Panel
NDU	National Defense University
NORAD	North American Aerospace Defense Command
NRO	National Reconnaissance Office
NSA	National Security Agency
NSAID	National Security and International Affairs Division
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
PEO	Program Executive Officer
PM	Program Manager
POM	Program Objective Memorandum
QDR	Quadrennial Defense Review
SAIC	Science Applications International Corp.
SASC	Senate Armed Services Committee
S&I	Survey and Investigations (HASC)

USD(A&T)	Under Secretary of Defense (Acquisition and Technology)
VCJCS	Vice Chairman of the Joint Chiefs of Staff

PPWF

ISBN 1-879716-58-5