PUBLICATION

Interoperability: Is It Achievable?

Anthony W. Faughn

October 2002

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.

Anthony W. Faughn, Lieutenant Colonel, U.S. Air Force, is deputy chief, Combat Systems Division, Communications and Information Systems Directorate, Headquarters Air Combat Command, Langley, Virginia. His previous assignments included serving as chief, communications and information branch, U.S. Nuclear Command and Control System Support Staff; commander, 613th Air Communications Squadron; and director, command, control, communications, computers, and information systems, Headquarters, 13th Air Force. He prepared this report while serving as an Air Force National Defense Fellow with the Program in 2000–2001.

ISBN 1-879716-84-4 P-02-6

October 2002

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Inc.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Sonexis
Strategy Assistance Services
TOR LLC
United States Government:
Department of Commerce
National Telecommunications and Information Administration
Department of Defense
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
Upoc
Verizon

Acknowledgments

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 Anderson
Opie Dawson, Esq.
Darryl C. Dean
Paul C. Fang
Oswald H. Ganley
Alan L. Jakimo
Thomas Julian
Donald Latham
P. H. Longstaff
Herbert Marks
Peter G. Neumann
Ron Ohs
William A. Owens
David C. Richardson
Robert A. Rosenberg
Stephen Sloan
James D. Smith, II
Scott A. Snook

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 also like to thank Dean R. Clemons, my successor as the Air Force National Defense Fellow at the Program, for his advice, Margaret S. MacDonald for her editorial guidance, and both of them for their friendship. My wife Katie and my son Zach deserve special gratitude for their patience and support when my work on this paper cut into my limited time with them.

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.

Executive Summary

The shortfalls in interoperability among U.S forces, first publicized by the press at the time of the Grenada invasion, became the catalysts for legislation and changes in defense policy, guidance, and procedures, and for numerous attempts to ensure joint interoperability. Despite tremendous planning and expenditure of funds, true interoperability, especially in the theaters with the greatest potential for conflict, continues to elude the Department of Defense [DOD].

This report presents a short, accessible account of the major issues associated with achieving interoperability. It first defines interoperability and addresses its relationship to other terms with which it is often confused: compatibility and integration. It then discusses the importance of interoperability as revealed by a review of lessons learned from past operations.

At the heart of the report are discussions of seven key factors that hamper the achievement of interoperability. These factors include the complex military acquisition culture; the shrinking defense budget; the effect of rapidly changing technology on maintaining interoperability among multiple generations of command-and-control (C2) and weapon systems; and the changing nature of operations, with the new emphasis on multinational operations. Although the DOD has little control over these four factors, it still needs to find the best possible responses to them. However, the department does have the authority and capability to adjust the balances among competing priorities and to alter its procedures for oversight and training. The DOD needs to enforce its requirements for certifying interoperability among systems and to conduct more frequent and more realistic military training and exercises, so that shortcomings in interoperability can be revealed and remedied.

The report next describes the impact of the DOD's recent revisions to three related policy and guidance documents and of the organizational changes that have given Joint Forces Command the mandate to enforce jointness among military C2 systems. Although complete interoperability will almost certainly never be achieved, the DOD's decisions at the beginning of the twenty-first century hold the key to improving interoperability in the future.

Contents

Chapter One

Interoperability: An Introduction

> *In the 1960s, the Sixth Fleet Commander, Admiral Kidd in the Mediterranean, used to die for information. The system was clogged up. He couldn't get information. Then every day he used to see this plane flying over the Mediterranean. It was an Air Force reconnaissance plane. It used to dip its wings to him. That plane had all the information he needed. They couldn't talk. Simple solution and a couple of young officers got medals. They put a compatible communications system on the plane and the ship. They solved it. The people thought they were heroes. Twenty years later, the same problem. A different part of the world; Air Force planes flying over a Navy ship; they couldn't talk to each other. You fix it by doing the same thing that was done 20 years ago. We sometimes just don't learn our lessons about communications problems.*
>
> — Fred R. Demech, Jr.[1]

1.1 Background

During the invasion of Grenada in 1983, the U.S. military encountered the same impediments that had exasperated Admiral Kidd twenty years earlier. The shortfalls in interoperability among U.S forces, publicized by the press at the time, became the catalysts for legislation and changes in policy, guidance, and procedures, and for numerous attempts to resolve issues that blocked the long road toward joint interoperability.

According to a memorandum issued in December 2000 by the under secretary of defense (USD) for acquisition, technology, and logistics; the assistant secretary of defense for command, control, communications, and intelligence (ASD C3I); the Department of Defense (DOD) director of operational test and evaluation; and the director of the Joint Staff:

> Despite long-standing existence of DoD policy on interoperability and a process for interoperability certification, interoperability problems persist. A report on the 1999 Operation Allied Force (Kosovo) cited numerous combined-interoperability problems. A General Accounting Office (GAO) report identified weaknesses in the DoD's interoperability certification process. The Commanders-in-Chief (CINCs) of the Unified Commands have frequently raised interoperability issues via the Joint Staff's Joint

---

[1]Fred R. Demech, Jr., "Making Intelligence Better," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1987* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-88-1, May 1988), 134, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/demech\demech-i88-1.pdf

Warfighting Capability Assessment (JWCA) process, the CINC Interoperability Program Offices (CIPOs), and other fora.[2]

To those within the military services, and perhaps especially to those outside them, it seems nearly incredible that problems with interoperability persisted in Kosovo after all the effort and money spent in the fifteen years since the fiasco in Grenada. How did these problems evolve? Why are CINCs and service staffs still concerned with interoperability?

Interoperability was not a significant concern during World War II, largely because the United States had essentially no military equipment when it entered the war. The government had to purchase practically all materiel at the same time and naturally bought the same equipment for all the services—whether it was ultimately to be fielded in ships, tanks, or airplanes. By default, therefore, the services achieved interoperability.[3]

In the fifty-plus years since the War, budget constraints have meant that the U.S. military services could not completely replace all their systems at once, as impractical as that would be to do even if they had the money and wanted to do it. Instead, each service procured individual systems that optimally supported its own activities at particular times. This approach resulted in different generations of equipment that did not interoperate with the materiel and systems of the other services. It caused little or no difficulty, and may even have improved performance at a time when the services operated more or less independently. With the advent of joint operations, shortcomings in interoperability became all too apparent.

Lessons learned from joint U.S. operations in the 1980s and 1990s—Grenada, the Persian Gulf War, Somalia, Rwanda, Liberia, Bosnia, and Kosovo—and debates over their degree of success all emphasize insufficient interoperability among the services and between U.S. and allied or coalition forces. Despite the tremendous planning and expenditure of funds to ensure interoperability, major problems remain in the theaters with the greatest potential for conflict. The issue does not go unrecognized. *Joint Vision 2020*,[4] published in June 2000, mandates interoperability; the CINCs of the unified and specified commands, the four service chiefs, and members of Congress all espouse its importance. In addition to being an important goal in its own

---

[2]Jacques S. Gansler, Arthur L. Money, Philip E. Coyle, and Scott A. Fry, Memorandum for Secretaries of the Military Departments, USD for Policy, USD (Comptroller/Chief Financial Officer), ASD for Legislative Affairs, General Council, Subject: Promulgation of DOD Policy for Assessment, Test, and Evaluation of Information Technology System Interoperability, Dec. 4, 2000.

[3]David W. Phillips, interview with author, Joint C4ISR [Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance] Decision Support Center, Crystal City, Va., Jan. 19, 2001.

[4]Chairman of the Joint Chiefs of Staff [CJCS], *Joint Vision 2020* (Washington, D.C.: U.S. Govt. Printing Office, June 2000), [On-line]. URL: http://www.dtic.mil/jv2020.html This is the most recent version of the vision statement that the CJCS is required to develop to provide overarching guidance to the armed forces.

right, interoperability is one of the most important building blocks of "information superiority," which the DOD views as key to achieving the goals stated in *Joint Vision 2020*.[5]

Numerous DOD efforts, such as the ongoing 2001 Quadrennial Defense Review (QDR), focus on achieving interoperability. Since 1998, in attempts to mitigate the effects of factors that hamper interoperability, the DOD has promulgated policy and guidance; redefined organizational roles, such as that of Joint Forces Command (JFCOM); and implemented evolutionary acquisition processes.[6] Although several years may need to pass to determine their effectiveness, these approaches remain relevant to the current discussion, because they will guide the DOD's attempts to attain interoperability.

1.2 Scope and Organization

Despite the many programs and activities that have been instituted to achieve interoperability among the U.S. services, finding a concise document dedicated to the issue is nearly impossible. Only three studies conducted since computer technology became ubiquitous are directly associated with interoperability. The first was carried out for the DOD by the Institute for Defense Analyses (IDA) and published in 1976. Though declassified and still amazingly relevant, this document is not releasable outside the IDA. The second, a report on a study conducted by the National Research Council (NRC) at the direction of Congress in 1996 and completed in 1999,[7] is lengthy and technical. The third, a report in the RAND Corporation's Project Air Force series,[8] deals almost exclusively with interoperability between the U.S. Air Force and coalition forces. The objective of the present report, in the absence of any hard documentation of problems of interoperability in the services on which to draw, is a short, accessible account of the major issues associated with achieving interoperability.

Following this introduction, **Chapter Two** defines interoperability and addresses its relationship to other terms with which it is often confused: compatibility and integration.

---

[5]U.S. Department of Defense, *Information Superiority: Making the Joint Vision Happen* (Washington, D.C.: Office of the ASD C3I, 2001). For a detailed analysis of information superiority and the role of interoperable systems, see Walter P. Fairbanks, *Information Superiority: What Is It? How to Achieve It?* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-99-4, June 1999), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/fairban\fairban-p99-4.pdf

[6]For a discussion of evolutionary acquisition, see **Section 5.3**.

[7]National Research Council, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy Press, December 1999), [On-line]. URL: http://books.nap.edu/books/0309064856/html/R15.html (hereafter referred to as the NRC report). (Accessed on Nov. 6, 2000.)

[8]Myron Hura, Gary McLeod, Eric Larson, James Schneider, Daniel Gonzales, Dan Norton, Jody Jacobs, Kevin O'Connell, William Little, Richard Mesic, and Lewis Jamison, *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, Calif.: The RAND Corp., 2000).

Chapter Three sets the stage by discussing the importance of interoperability as revealed by a review of lessons learned from past operations. The chapter also describes the continued importance of interoperability to joint operations and senior leadership, and its impact on future operations. **Chapter Four,** which constitutes the heart of the paper, identifies and analyzes factors that contribute to or hamper the achievement of interoperability. It describes the effects of rapidly changing technology, the changing nature of operations, competing priorities, inadequate oversight, and poor joint training and exercises. **Chapter Five** presents mitigating initiatives that the DOD undertook in 1999–2001 to improve interoperability among the services, including changes in policy and guidance, organizational roles, and acquisition processes. **Chapter Six** summarizes the discussion and draws conclusions as to whether, given past experience, the DOD initiatives may be expected to resolve the interoperability dilemma, or even to bring about any significant improvements.

Chapter Two

Definitions

The difficult and complex nature of achieving interoperability among command, control, communications, and computer [C4] systems can be seen in the Directorate of C4 Systems' recommendation that program managers evaluate and assess eleven separate references as they try to determine if C4I can achieve interoperability by 2020.[1] This author has chosen to use the definitions given in the following paragraphs for the purposes of this report.

2.1 Operational and Technical Definitions

Joint Publication 1-02, the *DOD Dictionary of Military Terms*, serves as the core document to which the services and agencies refer for official definitions. It defines interoperability in the following ways:

> Interoperability—1. (DoD–NATO) The ability of systems (units, or forces) to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. (DoD Only) The condition achieved among communications–electronics equipment when information services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.[2]

---

[1]Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 3170.01B, *Requirements Generation System* (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, April 15, 2001); CJCSI 6212.01B, *Interoperability and Supportability of National Security Systems (NSS), and Information Technology Systems (ITS*), (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, May 8, 2000); DOD Instruction [DODI] 5000.1, *The Defense Acquisition System (Change 1)* (Washington, D.C.: Office of the Secretary of Defense, Jan. 4, 2001); DODI 5000.2, *Operation of the Defense Acquisition System (Including Change 1)* (Washington, D.C.: Office of the Secretary of Defense, Jan. 4, 2001); DOD Regulation 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs* (Washington, D.C.: Office of the Secretary of Defense, June 10, 2001); DOD Directive 7045.14, *Planning, Programming, and Budgeting System (PPBS)*, *Change 1* (Washington, D.C.: Office of the Secretary of Defense, July 28, 2001); DOD Directive 2010.6, *Standardization and Interoperability of Weapons Systems and Equipment Within the North Atlantic Treaty Organization* (Washington, D.C.: Office of the Secretary of Defense, March 5, 1980); CJCSI 2700.01, *International Military Rationalization, Standardization, and Interoperability Between the United States and Its Allies and Other Friendly Nations* (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, Jan. 30, 1995); DOD Directive 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems* (Washington, D.C.: Office of the Secretary of Defense, Nov. 12, 1992); and DODI 4630.8, *Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems* (Washington, D.C.: Office of the Secretary of Defense, Nov. 18, 1992).

[2]Joint Publication 1-02, *Department of Defense Dictionary of Military Terms* [as amended] (Washington, D.C.: U.S. Govt. Printing Office, Dec. 7, 1998), [On-line]. URL: http://www.dtic.mil/doctrine/jel/doddict

The 1999 report of the congressionally mandated study *Realizing the Potential of C4I: Fundamental Challenges* expands on these definitions by discussing the terms operational and technical interoperability: "Operational interoperability addresses support to military operations and, as such, goes beyond systems to include people and procedures, interacting on an end-to-end basis." With regard to technical interoperability, it states: "Interoperability at the technical level is essential to achieving operational interoperability"; and interoperability is "an issue that arises between two systems rather than organizations."[3] Even though the 1999 report does not represent the official views of the DOD, the implications are useful in understanding the dimensions of interoperability.

Technical interoperability stops at the systems. If two or more systems can exchange data, then they are considered technically interoperable. By contrast, *operational* interoperability adds the user and assumes that the information exchange is between two or more users (senders and receivers), who must be able not only to exchange information but also to understand it. "Understand" is the key word. For example, it does no good for a German commander to exchange information with a U.S. counterpart unless the German officer can read and speak English, or vice versa. To achieve operational interoperability, the information must be converted at each end, so that it is understandable to both parties; in other words, they must use the same coding scheme.

2.2 Relationship to Compatibility and Integration

Because the terms "compatibility" and "integration" occur so frequently in discussions of interoperability, they are sometimes considered synonymous with interoperability and can confuse the discussion. Joint Publication 1-02 defines compatibility as the "capability of two or more items or components of [C4 system] equipment or material to exist or function in the same [C4] system or environment without mutual interference,"[4] while, for computing, Federal Standard 1037C defines compatibility as "the ability to execute a given program on different types of computers without modification of the program or the computers."[5] The Institute of Electrical and Electronic Engineers (IEEE), which sets the standards for much of the industry, defines integration as "The merging or combining of two or more lower-level [C4 system]

---

[3]National Research Council, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy Press, December 1999), Chapter Two, 1, 2, [On-line]. URL: http://books.nap.edu/books/0309064856/html/64.html (Accessed on Nov. 6, 2000.)

[4]Joint Publication 1-02, *Department of Defense Dictionary of Military Terms* [as amended] (Dec. 7, 1998).

[5]National Communications System, Technology and Standards Division, *Federal Standard 1037C, Telecommunications: Glossary of Telecommunications Terms* (Washington, D.C.: General Services Administration, Aug. 7, 1996), [On-line]. URL: http://www.its.bldrdoc.gov/fs-1037/ (Accessed on Aug. 20, 2002.)

elements into a functioning and unified higher-level [C4 system] element with the functional and physical [C4 system] interfaces satisfied."[6]

Rear Admiral Robert M. Nutwell, deputy secretary of defense for command, control, communications, and intelligence, surveillance, and reconnaissance systems, explained these related concepts in the following way:

> Integration is generally considered to go beyond mere Interoperability to involve some degree of functional dependence. For example, a mission planning system might rely on an external intelligence database; an air defense missile system will normally rely on acquisition radar. While interoperable systems can function independently, an integrated system loses significant functionality if the flow of services is interrupted. An integrated family of systems must of necessity be interoperable, but interoperable systems need not be integrated.
>
> Compatibility is something less than Interoperability. It means that systems/units do not interfere with each other's functioning. But it does not imply the ability to exchange services. Interoperable systems are by necessity compatible, but the converse is not necessarily true. To realize the power of networking through robust information exchange, we must go beyond compatibility.
>
> In sum, Interoperability lies in the middle of an "Integration Continuum" between compatibility and full integration. It is important to distinguish between the fundamentally different concepts of compatibility, interoperability, and integration, since failure to do so sometimes confuses the debate over how to achieve them. While compatibility is clearly a minimum requirement, the degree of interoperability/integration desired in a Joint family of systems or units is driven by the underlying Operational Concept, as well as by Family of Systems (FoS) design and cost/effectiveness tradeoffs.[7]

These differences are important, not only technically but also operationally, because the differences between compatible, interoperable, and integrated can affect operations. This report uses Admiral Nutwell's definitions.

---

[6]Institute of Electrical and Electronics Engineers, *IEEE Standards Collection—Software Engineering* (Piscataway, N.J.: IEEE, 1994).

[7]National Research Council, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy Press, December 1999), Chapter 2, 1, 2, [On-line]. URL: http://books.nap.edu/books/0309064856/html/R15.html (Accessed on Nov. 6, 2000.)

Chapter Three

The Importance of Interoperability

3.1 Operations over the Past Two Decades and the Future

A look at U.S. joint operations in the 1980s and 1990s reveals the importance of interoperability. Although Grenada drew attention to the inadequacies in interoperability, interoperability was an important goal even before the invasion. In 1982, Hillman Dickinson, then the director of C3 systems for the JCS, listed "improve joint and combined interoperability" as the second of eight priorities, "because the services have to work together if we have to fight; you can't fight separately."[1] Little did he know that the validity of this statement would be demonstrated in an actual operation less than a year later.

3.1.1 Grenada

The short-notice decision in 1983 to deploy forces jointly to Grenada, taken in response to a perceived crisis, left each military service no time to develop mechanisms for communicating with the other services. The joint forces, constructed on an ad hoc basis, faced the need to achieve interoperability essentially on the fly. Reports that appeared in the media almost as soon as the mission ended, and subsequent congressional testimony by military leaders, showed that the U.S. forces largely failed to do so. Although many of the specific incidents reported, and the remedies suggested to prevent them from recurring in the future, have never been confirmed in the unclassified official literature, some unclassified lessons learned[2] acknowledged the problems:[3]

> The final challenge to invading forces was the lack of a fully integrated, interoperable communications system.… Communications was to have been the glue that would tie together the operation of the four independent United States military service elements. Unfortunately, communications support failed in meeting certain aspects of the mission.… For example, uncoordinated use of radio frequencies caused a lack of interservice communications except through offshore relay stations and prevented radio communications between Marines in the north and Army Rangers in the south. As such, interservice communication was prevented, except

---

[1]Hillman Dickinson, "Planning for Defense-Wide Command and Control," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1982* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-82-3, December 1982), 23, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/dickins\dickins-i82-3.pdf

[2]The military services document lessons learned after each exercise or operation in a formal report as well as in the DOD's Joint Universal Lessons Learned System.

[3]Frank M. Snyder, *Command and Control: The Literature and Commentaries* (Washington, D.C.: National Defense University Press, 1993), 111.

> through offshore relay stations, and kept Marine commanders unaware for too long that Rangers were pinned down without adequate armor. In a second incident, it was reported that one member of the invasion force placed a long distance, commercial telephone call to Fort Bragg, N.C., to obtain C-130 gunship support for his unit which was under fire.… Commenting overall on the issue of interoperability, Admiral Metcalf [the CINC of Atlantic Command and the overall commander for the operation], wrote, "In Grenada we did not have interoperability with the Army and the Air Force, even though we had been assured at the outset that we did."[4]

These and other revealed shortcomings in interoperability raised widespread concern in the DOD, prompting the secretary of defense to issue an instruction on interoperability and the JCS to produce a memorandum of policy on the same subject. The need of the military to remedy a situation that could cost lives, coupled with the bad publicity at the time, may have contributed to the congressional concerns that led to the DOD Reorganization Act of 1986 (also known as the Goldwater–Nichols Act), which redefined the relationship between the services and the CINCs.[5] In 1985, Donald Latham, the former ASD C3I, commented:

> …if you want to talk across services (and that came up in Grenada, about cross service communications with different types of radios, using different types of COMSEC equipment) you're probably going to be in trouble.… However, we do have a new program called Joint Interoperability of Tactical Command and Control Systems (JINTACCS) which is a joint, cross service effort to make sure that tactical command and control systems are, in fact, interoperable. We will spend about $100 million on that in 1986 doing tests, promoting standards, setting up various testbeds, doing simulations, and trying to be the keepers of the interoperability.[6]

Five years later, this program was tested in the aftermath of Saddam Hussein's invasion of Kuwait.

---

[4]Stephen Anno and William E. Einspahr, "The Grenada Invasion," in *Command and Control Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid* (Maxwell Air Force Base, Ala.: Air University Press, Air War College Research Report, No. AU-AWC-88-043, 1988) [reprinted as an extract from the original report by the U.S. Naval War College Operations Department, NWC 2082], 40, 42 [On-line]. URL: http://www.fas.org/man/dod-101/ops/urgent_fury.htm (Accessed on Feb. 5, 2001.)

[5]Snyder, 111.

[6]Donald Latham, "A View from Inside OSD," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1985* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-86-1, February 1986), 121, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/latham\latham-i86-1.pdf

3.1.2 Persian Gulf War

Desert Shield and Desert Storm provided real-world tests of the ability of U.S. forces to operate jointly as codified in the Goldwater–Nichols Act, as well of equipment designed to ensure interoperability. As in Grenada, the missions suffered from the lack of interoperability among the U.S. forces, a reality acknowledged by then Secretary of Defense Richard Cheney in his interim and final reports to Congress.[7] In a book on the essential literature in command and control (C2), Frank M. Snyder, a retired Navy captain and professor emeritus at the Naval War College, identified the interim report on C3 systems in Desert Storm as providing especially valuable guidance regarding interoperability:

> …it is fresher, more informative, and covers the issues more frankly…. The general tone is one of accomplishment, even claiming for the C^3I system much of the success of Desert Storm. Yet despite the upbeat language, it is clear that greater attention will need to be paid to plans for…a greater measure of interoperability.[8]

Similarly, former Secretary of Defense Les Aspin and former Representative William Dickinson, in their *Defense for a New Era, Lessons Learned of the Persian Gulf War*, pointed out the pervasive lack of adequate interoperability:

> Operation Desert Storm demonstrated that tactical communications are still plagued by incompatibilities and technical limitations. At CENTCOM [U.S. Central Command] corps and wing levels, a significant portion of the war was conducted over commercial telephone lines because of the volume and compatibility limitations of the military communications system…. Communications were worse in the field….[9]

Particular difficulties arose with the tri-service tactical (TRI-TAC) communications equipment, acquired beginning in the late 1970s and fielded in the 1980s in an effort to guarantee interoperability. The Army's unclassified lessons learned devoted considerable attention to a serious problem stemming from the difference in the planning tools used by the Air Force and the joint community and those used by the Army in setting up the TRI-TAC communications architecture hubs—the circuit and message switches that provided the command and control backbone. The Army used the acquisition program's objective (or desired) network planning and

---

[7]U.S. Secretary of Defense, "Command, Control, Communications, and Operational Security of the Coalition Forces as a Whole; and Command, Control, Communications, and Operational Security of the United States Forces," Question 15, in *Conduct of the Persian Gulf Conflict: An Interim Report to Congress* (Washington, D.C.: Office of the Secretary of Defense, 1991); U.S. Secretary of Defense, *Conduct of the Persian Gulf War: Final Report to Congress* (Washington, D.C.: Office of the Secretary of Defense, April 1992).

[8]Snyder, 79.

[9]Ibid., 71.

management tool, which in July 1990 had undergone and successfully passed a User's Acceptance Test. Owing to the constraints on the physical space required to transport the system that incorporated the objective tool, the Air Force and joint community chose not to use it and instead adopted another tool as their interim solution. This almost completely prevented the electronic exchange of network planning and management products between the Army and Air Force. It therefore slowed information sharing; created inconsistencies in products required to ensure that all the services were using the same system configurations, such as circuit routing lists, circuit and message switch databases, and theater-level network diagrams; and prevented publication and use of a common theater telephone directory.[10]

The Army also highlighted further incompatibilities associated with the concept of joint forces:

> There was no data conversion and translation between the information received via JTIDS [Joint Tactical Information Distribution System] in the AWACS [Airborne Warning and Control System] for transmission on the TADIL-A [Tactical Digital Information Link] net. Conversely, information received via TADIL-A in the AWACS was not available for conversion to the JTIDS net.[11]

Thus, the AWACS could not relay information it received through one system on another system.

The Navy echoed the Army's concerns. According to the Navy's unclassified lessons learned, "problems were encountered, particularly in command and control, communications, [and] interoperability…."[12] For example, the joint forces air component commander in charge of prosecuting the air war and of all services' airplanes and air taskings used the air tasking order (ATO) as a centralized planning and execution tool, and this proved effective in managing the vast number of sorties generated to concentrate coalition airpower against Iraq; but "there were some problems with production of the ATO and its delivery to naval forces."[13] The Navy was unable to receive the ATO electronically, which meant that the ATO had to be printed and then delivered to the fleet by helicopter.

---

[10]Center for Army Lessons Learned [CALL], "Interoperability," in *Joint Tactical Communications (TRI-TAC)*, CALL Newsletter 92-1 (January 1992), [On-line]. URL: http://call.army.mil/products/newsltrs/92-1/92-1ch3.htm (Accessed on Nov. 2, 2000.)

[11]Ibid.

[12]U.S. Dept. of the Navy, "Lessons Learned and Summary," in *U.S. Navy in Desert Shield/Desert Storm*, *Quick Look: First Impressions Report* (Washington, D.C.: U.S. Dept. of the Navy, Naval Historical Center, March 22, 1991), 1, [On-line]. URL: http://www.history.navy.mil/wars/dstorm/ds6.htm (Accessed on Jan. 2, 2001.)

[13]Ibid.

3.1.3 African Operations in the 1990s

The African operations of the 1990s illuminated the difficulty in interoperability among multinational forces, especially with those of developing countries and international organizations associated with the changing nature of military operations and operations other than war. Lessons learned from Operation Restore Hope (Somalia, 1991) emphasized such challenges:

> The most significant potential of interoperability problems occurred between U.S. forces and the multinational contingents…. Equipment considered standard—even basic—in most western armies is simply not present in the inventories of many military contingents from developing countries.… The equipment multinationals do bring with them is not likely to be interoperable.… [C]rossing over the "seams" of national control created severe interoperability problems—a situation that occurred whenever one national contingent had to cross over the boundary to reinforce another.[14]

Somalia also revealed barriers to interoperability among U.S. forces. The lessons learned noted that, "The internal problems affecting U.S. forces did not involve any Grenada-like operational fiascoes; however, the ones that did occur underline the continuing problem of aligning equipment, procedures, and standards in the joint environment."[15] The Marine Amphibious Ground Task Force, an organization set up and staffed by the Marine Corps, used an obscure word-processing software, while CENTCOM, like most other military users, preferred a more modern package. At headquarters, a similar difficulty plagued exchanges of electronic mail (e-mail). At the tactical level, the ATO formats differed for east and west coast ships of the Marine Amphibious Ready Group. The most serious instance reported was that although the Army and Marines used the same single-channel tactical radios, they used different upgrades, resulting in an incompatibility severe enough to prevent the Army hospital in Mogadishu from being able to talk to the Navy offshore for the first three weeks of the operation.[16]

Three years later, in Rwanda, the lessons learned identified similar challenges to interoperability in dealing with multinational forces as well as with private volunteer organizations and nongovernmental organizations:

> Although organizations were adept at intraorganizational communications procedures, interorganizational communications dragged because of dissimilar communications equipment, platforms, frequencies, and protocols. The lack of interoperable hardware and peripherals, common

---

[14]C. Kenneth Allard, "Operational Lessons Learned," in *Somalia Operations: Lessons Learned* (Washington, D.C.: National Defense University Press, 1995), 1, 6, [On-line]. URL: http://www.ndu.edu/inss/books/allardch2.html

[15]Ibid., 23.

[16]Ibid., 24.

> standards, and protocols was the main obstacle to looped communications and to reliable and broad-based security in the field.[17]

The same problems plagued operations in Liberia in 1996. A 1997 conference on "Managing Communications: Lessons from Interventions in Africa," which brought together representatives from U.S. civilian government agencies, the U.S. and United Nations militaries, and nongovernmental organizations, generated lessons learned that focused on the cost involved in achieving interoperability with emerging nations. Participants emphasized that "Lack of funding for communications will further exacerbate this situation…. Although lateral [unit-to-unit] communications in the field seem imperative, the lack of interoperability continues to impede communications, whether by radios or computers."[18]

3.1.4 Operation Desert Fox

In 1998, seven years after Desert Shield/Desert Storm, the United States found itself once more engaged in combat actions against Saddam Hussein and Iraq in Operation Desert Fox. Interoperability still eluded achievement. Desert Fox also showed that despite improvements to and dependence on technology, a minor technical problem, or "glitch," could have a significant impact. This time the hindrance to interoperability came from the common operational picture intended to give the operational commander an overview of the battlespace and forces—even though providing that picture had been an important focus of programs since Desert Storm. A CNN article captured the significance and potential impact of the "small glitch" in the Global Transportation Network (GTN), the system that allows the military leadership to maintain in-transit visibility (ITV), that is, constant knowledge of the movements of troops and equipment throughout the world:

> Because of a glitch…GTN presented military planners at three commands with two different operational pictures…. Although GTN was designed to automatically process updates within 30 seconds, a software problem such as the one experienced in Desert Fox could cause a significant drop in responsiveness and hinder the ability to make "on the spot" decisions…. The problem occurred when a data field from the Joint Operations and Planning System (JOPES)—a multiservice system that provides the military with a standard format and language for planning military operations—failed to convert properly when it reached GTN. This failure presented planners with false information on the status of cargo aircraft…. Although GTN never went down, the interoperability problem caused some confusion when the Air Mobility Command (AMC) and U.S. Central

---

[17]Stanley Roth, "Conference Summary," in *Managing Communications: Lessons from Interventions in Africa* (Washington, D.C.: U.S. Institute of Peace, March 1997), 29, 31 [On-line]. URL: http://www.usip.org/oc/sr/managingcomm4.html (Accessed on Jan. 2, 2001.)

[18]Ibid., 31.

> Command were working with different information than TRANSCOM [U.S. Transportation Command] was using…. If GTN were to fail, users would be forced to resort to the use of fax machines, phones and other manual methods, and users would have to make do with old information.
>
> Martin Libicki, a defense analyst with Rand Corp. specializing in information warfare and information operations, said he was surprised that a small glitch such as the one with the JOPES-GTN interface could happen, given the state-of-the-art technology. "We've been doing this [database technology] for years," he said.[1]

3.1.5 Kosovo

The Kosovo mission, Operation Allied Force, which began in 1999, offered the latest example of shortfalls in interoperability under combat conditions. In particular, it revealed the growing gap in interoperability between the U.S. and allied or multinational forces. Although documented problems associated with U.S. interservice interoperability remained, the lessons learned emphasize primarily the growing difference in technology between the United States and its allies.

In a joint statement to the Senate Armed Services Hearing on Kosovo, the senior leadership of both the U.S. and North Atlantic Treaty Organization (NATO) forces identified interoperability as an impediment among the allied troops. General Wesley Clark, NATO Supreme Commander, Admiral James Ellis, Commander of Allied Forces–Southern Europe, and Lieutenant General Michael Short, Commander of Allied Forces–Central Europe, had this to say:

> Finally, Operation Allied Force illuminated the capability gaps between the U.S. military and our NATO allies. For example, not all NATO nations possess adequate…secure communications…. These gaps impeded interoperability among Allied forces during the campaign…. Ultimately, NATO nations need to upgrade their militaries to ensure they remain compatible with U.S. Forces.[2]

---

[1]Daniel Verton, "Software SNAFU Slowed Key Data During Iraqi Raid," CNN, Feb. 25, 1999, [On-line]. URL: http://cnn.com/TECH/computing/9902/25/iraqi.idg/index.html (Accessed on Nov. 9, 2000.) Martin C. Libicki is also the author of several books and articles on the impact of technology on national security, including *Standards: The Rough Road to the Common Byte* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-94-6, August 1994), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/libicki\libicki-p94-6.pdf and "Information War: Ready for Prime Time?" in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1996* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-97-1, January 1997), [On-line]. URL:http://www.pirp.harvard.edu/pubs_pdf/libicki/libicki-i97-1.pdf

[2]U.S. Mission to NATO, "Joint Statement to Senate Armed Services Hearing on Kosovo: Lessons Learned," *The U.S. Mission to NATO Security Issues Digest*, 203 (Oct. 21, 1999), 6.

3.1.6 Future Operations and Wars

As the lessons learned from Kosovo indicate, the absence of interoperability will impede future NATO and European operations. The Pacific theater faces equal if not greater difficulties in the future.

An article published early in 2001, although Army-centric, highlighted overall interoperability problems in Korea and the Pacific theater, where the United States expects its forces may have to fight one of the two major theater wars[21] envisioned in the planning documents of the DOD. The article drives home the relevance of interoperability in a part of the world where the DOD has focused much of its planning since the 1950s and where the potential exists to be at war very quickly, giving deploying forces little time for preparation and requiring them to come as they are.

> Old, incompatible command and control systems are preventing the U.S. Army from sharing information in a timely manner with other regional services and allies.… These disparate systems, known as stovepipe systems, perform only one function and do not share information with other voice, video, and computer systems. This means Army leaders in the region must make decisions using data that sometimes is two to four hours old in an era when battlefield and intelligence information changes by the second, industry and military officials say.[22]

The article also cites the concerns of Lieutenant General Ed Smith, commanding general of U.S. Army Forces Pacific:

> U.S. Army Pacific Command (USARPAC), Honolulu, also receives untimely information from U.S. services and ally countries in the region because of its stovepipe C4 systems.… "We need to minimize the interoperability gaps," Smith said, "We need to think joint, not Army…. The Army should not think in terms of integrating its C4I systems service-wide, but rather linking its future systems with those of other services and countries," he said.[23]

Inadequate interoperability is not limited to the Korean peninsula. According to retired Army Brigadier General Jack Schmitt, "Inadequate C4I connections complicate Army interoperability with other countries in the Asia and Pacific theaters."[24]

---

[21]The national military strategy is based on being able to fight and win "two major theater wars (two MTWs)" nearly simultaneously. This strategy is the basis for the services' personnel strengths, budgets, and equipment acquisitions and procurements.

[22]Frank Tiboni, "Slow Systems Hinder U.S. Pacific Forces, Allies," *Defense News* **16**, 1 (Jan. 8, 2001), 12.

[23]Ibid.

[24]Ibid.

3.2 Continuing Importance of Interoperability

The United States no longer plans to fight in such a way that the individual services would each conduct their own operations, as they did in Korea or Vietnam. Instead, prompted in large measure by the lack of interoperability during the Grenada invasion, Goldwater–Nichols established that all future operations would be joint. This means that the forces will require joint C2, and that interoperability will be "a key enabler for the conduct of effective, collaborative, multi-service military operations."[25]

3.2.1 Joint Operations

According to Victor A. DeMarines, president of The MITRE Corporation from 1996–2000,

> True joint C2 requires not only that the force components from various services be able to communicate with the Joint Task Force headquarters, but that they also have effective tactical communications among each other.... Access to the Air Tasking Order should not require resorting to paper, as in DESERT STORM and Kosovo…. The first step toward a genuinely joint C2 system that fully leverages the potential of IT [information technology] is interoperability.[26]

As a result of the shift to joint operations, the visions, policy, doctrine, tactics, and procedures of the DOD have evolved to embrace interoperability. Both *Joint Vision 2010* and *Joint Vision 2020* advocate the necessity for interoperability. *Joint Vision 2020* reiterates the importance of interoperability for successful multinational and interagency operations. In dedicating a complete section of the short (thirty-six page) document to interoperability, it underscores the need to improve interoperability and establishes the mandate for doing so:

> Interoperability is the foundation of effective joint, multinational, and interagency operations. The joint force has made significant progress toward achieving an optimum level of interoperability, but there must be concerted effort toward continued improvement…. Interoperability is a mandate for the joint force 2020—especially in terms of communications … and information sharing…. [A]s with multinational partners,

---

[25]NRC, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy Press, December 1999), Chapter Two, 1,4, [On-line]. URL: http://books.nap.edu/books/0309064856/html/64.html (Accessed on Nov. 6, 2000.)

[26]Victor A. DeMarines, "Exploiting the Internet Revolution," in *Keeping the Edge: Managing Defense for the Future*, edited by Ashton B. Carter and John P. White (Cambridge, Mass.: MIT Press, 2001), 66. The MITRE Corporation is the Air Force's federally funded research and development center for C2 systems.

> interoperability in all areas of interaction is essential to interagency operations.[27]

3.2.2 Senior Level Focus

A key indicator of importance is where senior level staffs (e.g., the Office of the Secretary of Defense [OSD], the Joint Staff, etc.) focus their attention. In 1999–2001, top-level staffs dedicated significant effort to drafting, coordinating, and publishing updated policy concerning interoperability. For example, the DOD 5000 series of instructions, issued on January 4, 2001, which provide acquisition policies and guidance, and the June 2000 Chairman of the Joint Chiefs of Staff Instructions (CJCSIs) for the requirements process mandate a stringent requirements and acquisition process to ensure interoperability (see **Chapter Five**).

A look at the effort behind the production of *Joint Vision 2020* reveals the importance of interoperability. The underpinning of the Pentagon's new vision statement for what the military should be capable of achieving around 2020 was interoperability among the services. According to Marine Major General Henry Osman, the Joint Staff's director for operations, plans, and joint force development, "Interoperability is the foundation upon which all of our doctrine and systems have to be based in order to achieve Joint Vision 2020.… The force must be fully joint, intellectually, operationally and technically.... [We will fight] not as a single military service, but rather [as] the four services cooperating much more seamlessly."[28]

Ongoing work supports this view. For example, the 2001 QDR, an evaluation undertaken every four years by the DOD, focused on information superiority, particularly interoperability. Arthur Money, ASD C3I and the DOD's chief information officer [CIO] from October 1999 to April 2001, correctly predicted this in November 2000:

> Indeed, information superiority may become the crux of the 2001 QDR. Money said defense officials will likely address two main subsets of information superiority—interoperability and information assurance—in the QDR, focusing on speeding up the time it takes for commanders to obtain accurate information and make a decision.[29]

Brigadier General Lynn Hartsell, director of the Army QDR Office, echoed this position in a talk on Army QDR efforts, in which he placed special emphasis on feedback from the CINCs and the

---

[27]Chairman of the Joint Chiefs of Staff, "Vision Statement," in *Joint Vision 2020* (Washington, D.C.: U.S. Gov't. Printing Office, June 2000), 21.

[28]Hunter Keeter, "Joint Vision 2020 Should Reflect Better Interoperability, Official Says," *Defense Daily*, Oct. 13, 2000.

[29]Arthur Money, quoted in Anne Plummer, "Pentagon CIO Says Military Must Shift Focus to Information Superiority," *Inside the Pentagon* **16**, 48 (Nov. 30, 2000), 1.

Army's major commands[30] indicating that "Joint interoperability (especially C4ISR) is increasingly important."[31]

3.2.3 Warfighter and CINC Emphasis

The CINCs, whom Goldwater–Nichols considered the warfighters and who therefore possess tremendous power over the focus of the DOD's efforts, recognize that interoperability is fundamental. For example, the CINC for U.S. Space Command and commander of Air Force Space Command, General Ralph E. Eberhart, who is responsible for supporting all the regional, geographic, and other specified CINCs, underscored its importance in his 2001 Leader Policy Statement: "North American Defense (NORAD) today has some 25 computer systems, almost as many computer languages, and more than two million lines of software code to support. When you talk about reliability, maintainability, affordability, and you talk about interoperability, it is the real challenge."[32]

That the DOD designated a warfighting CINC as the advocate for joint interoperability demonstrates the significance it accords interoperability. In naming the Atlantic Command (ACOM) (renamed JFCOM in 1998) the force "integrator," the 1999 Unified Command Plan (UCP) assigned to it specific responsibilities to make certain that systems are interoperable and to conduct joint exercises and training aimed at improving interoperability. Since 1999, JFCOM, whose activities are discussed in **Chapter Five**, has been engaged in improving interoperability.

---

[30]The services are organized into major commands responsible for a particular geographic area or specific mission, such as the U.S. Army's U.S. Army Europe (USAREUR) and U.S Army Medical Command (MEDCOM) or the U.S. Air Force's U.S. Air Forces Europe (USAFE) and Air Force Space Command (AFSC).

[31]Lynn Hartsell, "The Army Quadrennial Defense Review," lecture to National Security Fellows, National Security Program, Harvard University, John F. Kennedy School of Government, Feb. 6, 2001, slide 8.

[32]Ralph E. Eberhart, USAF Leaders Policy Statements: Ryan, Peters, Eberhart, Lyles, Myers. E-mail from Capt. Timothy Cole, HQ USAF/XPS, Subject: News Clips, Feb. 6, 2001, 15.

Chapter Four

Factors Limiting Interoperability

It would be easy to fix the interoperability problem if one person, one office, or one institution could be held responsible. The situation did not occur over night, and the people, offices, and institutions involved have all changed several times, leaving no single person or entity to blame. Factors and combinations of factors contribute to the persistent shortcomings in interoperability, including the military acquisition culture, dwindling budgets, rapidly changing technology, the changing nature of operations, competing priorities, insufficient oversight, and unrealistic training and exercises. Although the DOD has little control over the first four factors, it still needs to find the best possible responses to them. It does, however, have the authority and capability to set priorities and to alter procedures for oversight and training.

4.1 The Acquisition Culture

The first factor that affects interoperability is the culture in which the DOD acquires major weapons and automated information systems. Just the number of organizations and people and the associated bureaucracy give a glimpse of the challenge. These include three under secretaries or assistant secretaries of defense charged with oversight; at least two Joint Staff directorates responsible for review of requirements, oversight, and certification; a minimum of two CINC staffs—the originating CINC and JFCOM as the advocate of interoperability; the service staff responsible for acquiring the system; and numerous defense agencies, including the Joint Interoperability Test Command (JITC), which is responsible for testing and certifying the system as interoperable. Add in Congress, defense contractors, and lobbyists and the inefficiency becomes apparent—and inevitable.

Ultimately, no one is in charge of the process. Although this situation may have come about by design and for good reason—to thwart any overzealous person or organization—it has led to a culture or environment with a significant, and unfortunate, impact on efforts to achieve interoperability.

4.2 Budgets

Another important contributing factor is the role of the budgeting process. The strengths and weaknesses of this process are beyond the scope of this report, but, suffice it to say that, although recent changes to the Requirements Generation System and Defense Acquisition System operations reflect (to varying degrees) the requirements of evolutionary acquisition and the necessity of interoperability, the Planning, Programming, and Budgeting System does not.[1] The

[1]James D. Smith, Carnegie Mellon University, private communication to the author, 2 Nov. 2001.

DOD's budget fell in the 1990s to the lowest percentage of gross national product in history. At the same time the demand for more information delivered more quickly has resulted in an increasing percentage of the budget spent on information systems. In November 2000, ASD C3I Arthur Money, also the Pentagon's CIO, estimated that the department was

> already spending anywhere from $75 billion to $100 billion a year on information technology—an estimation he said is nearly impossible to prove because so much of it is embedded within weapon systems and other defense programs. Providing resources to any of these activities, he said, is merely a "balancing act."[2]

Cheryl Roby, the deputy assistant secretary of defense for C3, programs and evaluation, stated early in 2001 that the tracked portion amounts to over 30 percent of the DOD's budget.[3] This constraint on resources sets the stage for fierce competition between major weapons systems and automated information systems. Additionally, within individual information systems programs the limited dollars intensify competition and force tradeoffs between interoperability and capability, such as more bandwidth or faster processors, or functionality, such as increased security. Such zero-sum games cannot be expected to result in cooperation among programs and, in fact, have not done so.

4.3 Rapidly Changing Technology

Rapid changes in technology have significantly hampered interoperability. Historically, the rate of change has been governed by what has come to be known as "Moore's law":

> Gordon Moore, a founder of Intel Corporation, observed in 1965 that the trend in the fabrication of solid state devices was for the dimensions of transistors to shrink by a factor of two every 18 months. Put simply, electronics doubles its power for a given cost every year and a half.
>
> In the three decades after Moore made his observation, the industry followed his prediction almost exactly.… Moore's law is not a "law" of the physical world. It is merely an observation of industry behavior. It says

---

[2]Anne Plummer, "Pentagon CIO Says Military Must Shift Focus to Information Superiority," *Inside the Pentagon* **16**, 48 (Nov. 30, 2000), 1.

[3]Cheryl J. Roby, "Threats Facing the Defense Department in the Twenty-First Century," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, November 2001), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/roby\roby-i01-3.pdf

> that things in electronics get better, that they get better exponentially, and that this happens very fast.[4]

It is easy to see the difficulties this rate of change poses for interoperability, given the unpredictability of what capabilities will be available even two years into the future, and the related problem of creating a new generation of systems every year and a half. Rapid technological change produces high (sometimes unrealistically high) expectations of new technology, creates legacy systems, and challenges the ability to develop and apply standards to promote interoperability.

4.3.1 Legacy Systems

As the generations of technology succeed one another, new systems must interface with "legacy" systems. The NRC report summarized this problem, noting that "the legacy systems issue is one of the greatest challenges faced by the DOD today."[5] It is financially and organizationally impossible for the DOD (or private industry, for that matter) to replace all of its computing systems, and the associated training and procedures, from the ground up every eighteen months. It is equally unrealistic for the U.S. armed services to ignore the potential advantages offered by the latest technologies, especially when potential adversaries have access to them. Real-world demands dictate that the military strike a balance between replacing all of its systems and "making do" by acquiring some new systems and devising ways to connect them with older machines.

The NRC report devoted considerable attention to the prevalence and seriousness of this problem:

> The military services have tended to retain legacy information systems that were developed in response to "stand-alone" requirements, were not regarded as subject to connection with other systems and, therefore, are not operationally friendly with their increasingly interdependent companion systems. The legacy systems issue is one of the greatest challenges faced by the DOD today. This base of information systems comprises thousands of multi-generation electronic system elements and billions of dollars of capital investment, and is kept alive through the expenditure of many more billions in support costs. In the commercial world, such legacy systems are often kept operational based on a view their cost must be amortized before new capability can be economically

---

[4]Robert W. Lucky, "Understanding Computers and Communications," in *The Information Resources Handbook*, edited by Benjamin M. Compaine and William H. Read (Cambridge, Mass.: MIT Press, 1999), 85–110, 87.

[5]NRC, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy Press, December 1999), Chapter Four, 19–20, [On-line]. URL: http://books.nap.edu/books/0309064856/html/64.html (Accessed on Nov. 6, 2000.)

> justified. The military environment likewise seeks to amortize its investment; but the reasons are both functional and economic: the large-scale modernization of legacy systems entails major changes in training, doctrine, and organization, in addition to the difficulty of securing political support for new investment dollars. [6]

For example, in 1987, when the DOD replaced the second-generation secure telephone unit system (STU-II) with the next-generation STU-III, the systems were not interoperable. Both had to be maintained until the late 1990s, when the STU-II was phased out.

Realistically, legacy systems will remain a fact of life for the military and will continue to plague interoperability. Recognizing this, the DOD needs to seek ways to achieve the maximum interoperability attainable. One way the military has attempted is by establishing common interface standards for systems.

4.3.2 Standards

The challenge of establishing and implementing standards for interoperability when technology is rapidly changing is daunting, not only to the DOD but also to industry.[7] Many believe that simply defining standards for interoperability makes interoperability easy to achieve. On the surface that makes sense: if an organization defines a technical parameter and all systems must comply with it, then it follows that the systems will be interoperable. In reality, this is much more difficult than it seems, because as technology changes so (naturally) do standards. Given the complexity of systems and the constant push to acquire the latest technology, defining standards for interfacing the new with the old or even the new with the new has proven tremendously complicated.

The DOD's effort to create a single integrated air picture (SIAP) serves as a good illustration of the technical difficulty associated with specifying standards for interoperability.

> In 1994, the ASD C3I promulgated a standard called "Link 16" and directed the services to move toward implementing it. However, the interoperability problem has proven too complex to be dealt with by means of a single standard. At present, the Link 16 standard consists of several hundred pages of detailed technical information, but it still requires interpretation and technical judgments. Because no organization or mechanism exists to coordinate the judgments made by the many different programs implementing Link 16, different systems comply with the

---

[6] Ibid.

[7] *Realizing the Potential of C4I*, Chapter Four, 21.

> standard different ways and cannot exchange data well enough to achieve a SIAP.[8]

The problem of establishing standards is not limited to complex systems, such as those associated with Link 16. A simpler example is the different e-mail programs used by the services. All the services can interface with one another while in garrison and connected with their local server, which is, in turn, connected with the Internet. When troops arrive at a deployed location with the same e-mail program they used in garrison and try to connect with the locally provided server, which uses a different suite or program, their e-mail cannot go through. As systems become technically more complex, the difficulty of defining standards does also.

Commercial industry's shift toward developing technology for the private sector rather than the military means that the DOD no longer enjoys the leverage it once had regarding the development and application of advanced information technology. Instead, the DOD needs to rely on commercial technologies.[9] Dependence on commercial off-the-shelf (COTS) equipment, coupled with the streamlining of the DOD's acquisition process to take advantage of the procurement of commercial items, complicates establishing standards.

The difficulty becomes apparent when weapons must interoperate with C2 systems. The DOD attempted to set standards in this area by requiring that commercial items used in C2 and weapons systems conform to two sets of standards for interfaces and interoperability—the Joint Technical Architecture (JTA) and the Defense Information Infrastructure/Common Operating Environment (DII/COE)—before they can be purchased. When acquisition programs tried to apply these standards, many of them have found that the standards severely constrain choice and that even terminology becomes a barrier. For example, one program found that less than 10 percent of the relevant data standards associated with the JTA matched data definitions employed in COTS items.[10] In response, the services added a variety of interfaces reflecting COTS terminology to the architecture, turning the JTA into a compilation of many different proprietary standards that did not interface with one another. As a result, a procured or acquired system could comply with the architecture but still not be interoperable with other JTA-compliant systems.

The DOD's demand for "open systems" standards capable of interfacing with the myriad manufacturers' systems represents another sticking point and an obstruction to applying commercial technology. The DOD values open systems, which use common interfaces instead of proprietary ones, because they act as enabling mechanisms to achieve the objective of interfacing several systems. Industry obviously wants to develop proprietary solutions to the demands of the

---

[8]DeMarines, 73.

[9]*Realizing the Potential of C4I*, Chapter Four, 38.

[10]OSD, *Commercial Item Acquisition—Considerations and Lessons Learned* (Washington, D.C.: Office of the Secretary of Defense, Discretionary - DOD Document, June 26, 2000), [On-line]. URL: http://web2.deskbook.osd.mil/reflib/DDOD/005EO/005EOdoc.htm (Accessed on May 29, 2001.)

market and regards open systems as an impediment to the protection of proprietary rights. In this vein, industry suspects the DOD of wanting to own the intellectual property rights for items developed under government contracts, because this would allow the DOD to turn those rights over to a contractor's competitors in order to create multisource competition for potential procurements. As the NRC report found, "This is unacceptable to industry in a world where intellectual property is regarded as the most important factor for survival against highly agile, fast-moving competition."[11]

The most complicated problem of all involves creating standards to promote interoperability between U.S and multinational or coalition forces (see section **4.4.1**). Martha Maurer, an active-duty Air Force colonel and author of one of the earliest books on coalition command and control, provides insight into the task of ensuring interoperability between coalition forces:

> The level of effective interoperability between coalition forces will affect command and control. Prior efforts to achieve interoperability were primarily focused on making functional areas of combat interoperable between U.S. Services. If that goal is applied to coalition forces, it indicates a need for common standards and procedures across the board.[12]

4.4 Changing Nature of Operations

The DOD has little control over the changing nature of warfare. The different military services historically conducted more or less autonomous operations (section **2.2**). The concept of fighting jointly was formalized in the Goldwater–Nichols Act of 1986 and further codified in joint doctrine and DOD directives. The trend toward multinational operations, started with Desert Shield/Desert Storm in 1990–91, reflects how the United States expects to conduct future operations.

As described in **Chapter Three**, these changes obviously bring with them challenges for interoperability—whether among U.S. forces or between U.S. forces and allied or coalition forces in multinational operations. The changing nature of operations has also altered the roles of various weapons systems and platforms, further challenging interoperability.

4.4.1 Multinational Operations

Problems of interoperability were prevalent among multinational forces even in Desert Shield/Desert Storm, which has been considered an overwhelmingly successful campaign. For example, the lessons learned included such statements as, "Multiservice strike packages were

---

[11] *Realizing the Potential of C4I*, Chapter Four, 22.

[12] Martha K. Maurer, *Coalition Command and Control: Key Considerations* (Washington, D.C.: National Defense University Press, 1994), 97.

difficult or impossible to assemble because various aircraft communicated in different ways over secure voice networks."[13] *Joint Vision 2020* emphasized that the United States expects to conduct operations not only as a joint U.S. force but also with allied and coalition forces and international organizations. As noted in section **3.1**, the lessons learned from Desert Shield/Desert Storm, the African operations of the 1990s, and the 1999 mission in Kosovo point out that the gap between U.S. technology and that of other countries causes an interoperability gap that affects the various allied forces. In an analysis of C2 issues, Frank Snyder emphasized the obstacles that multinational operations create:

> The achievement of interoperability for combined operations in which the forces of friendly nations are organized to operate and fight together is even more difficult. The command and control of a combined operation requires resolution of all the issues that arise in a joint operation, but in addition, requires coping with national intelligence and sources, as well as considerations of national pride. The interoperability problems that can arise during combined operations with Third World nations may be very great indeed.[14]

The NRC report emphasized the technical aspect of interoperability and illuminated issues associated with multinational interoperability. In addition to differences of language and doctrine, and uncertainty as to who U.S. coalition partners may be, the report identified various factors that make it difficult or "essentially impossible" to achieve interoperability among multinational coalitions. For example, "Potential coalition partners, for the most part, lack adequate resources to modernize their C4I systems, and thus may well be using equipment that is substantially incompatible with present and planned U.S. C4I systems." National pride leads most nations to favor indigenous military procurement of C4I systems, which reduces the likelihood that multinational systems will readily operate with U.S. systems. Last, with regard to security of information, the report stressed that the United States places many restrictions on the types of information it is willing to share with certain coalition partners, but it is difficult to develop interoperable information systems that allow only selective passage of information.[15] Multiply this requirement by the number of nations involved and the difficulty of building interoperable systems becomes overwhelming.

---

[13]Les Aspin and William Dickinson, *Defense for a New Era, Lessons Learned of the Persian Gulf War*, quoted in Frank M. Snyder, *Command and Control: The Literature and Commentaries* (Washington, D.C.: National Defense University Press, 1993), 71.

[14]Snyder, 112.

[15]*Realizing the Potential of C4I*, Chapter Four, 13.

4.4.2 Changed Roles of Weapons Systems

With changes in technology and in the nature of war come changes in the roles of some weapons systems. After the collapse of the Berlin Wall and the demise of the Soviet Union, several platforms built to deal with the nuclear threat of the cold war were tasked to perform new functions. For example, the B-1 bomber was assigned to a conventional (non-nuclear) bombing role, which changed the nature of its communications and interoperability requirements from strategic to tactical.

When new uses for old systems are discovered, a corresponding change or addition of interfaces is required. The recognition that the strategic warning system designed to detect and correlate a nuclear attack was capable of detecting launches of theater missiles resulted in an effort to adapt the system to provide warning at the tactical level. The new role significantly altered the types of communications systems, interfaces, and interoperability required for the warning systems to interface with theater tactical systems.

Another example is the military's preference for using standoff smart weapons, such as laser-guided missiles, that require instantaneous or continuous communication between the weapons and numerous systems for C2, guidance, and targeting information. Increased use of these weapons, rather than of more conventional platforms, and associated interface requirements create numerous challenges to interoperability. The growing demand for real-time intelligence and imagery, giving the pilot in the cockpit or soldier in the foxhole the latest images of the target or battlefield, also creates tremendous interoperability challenges.

This list could go on almost indefinitely. It is safe to surmise that continuing changes in the nature of war will only increase the challenges for interoperability.

4.5 Priorities

Although the DOD can only react to the factors discussed in sections **4.1** through **4.4**, it can initiate action to set and enforce priorities that promote the acquisition of interoperable systems and help to achieve interoperability among existing systems. Without fixed—and enforced—procedures, organizations, systems, and functions will continue to clash over conflicting priorities among requirements and funds.

The general principle that operational needs should drive the acquisition system is well established within the DOD. Under the traditional system, input from warfighters (based on the perspectives of the CINCs) is codified in terms of validated military requirements, which are vetted as the basis for undertaking a new program. The acquisition system takes the military

requirements and then—some years later—provides for fielding a system intended to meet them.[16]

4.5.1 Service versus CINC Priorities

According to Air Force Colonel Richard B. (Hoot) Gibson, director of the CINCs' Interoperability Program Office at the USAF Electronic Systems Center, "The problem is that while the Department of Defense assigns warfighter responsibilities to unified commands, each individual service is responsible for developing its own command and control systems…. This creates some big, ugly seams for joint commanders."[17] Indeed, interoperability frequently falls victim to the differing viewpoints of the CINCs and the services.

The experience of the U.S. Special Operations Command (SOCOM) offers a useful lesson regarding the importance of the priority assigned to interoperability:

> [A]s no surprise, a high degree of C2 interoperability and effectiveness is achievable if an organization is guided by joint priorities. Whereas the services procuring C2 systems for mainstream forces usually have other, higher priorities than interoperability with the other services or interoperability with all of the regional commands, SOCOM's priorities have been driven by its structure as a joint organization, and its recognition that it must retain the political support of the regional CINCs to survive.[18]

SOCOM enjoys the unique luxury of having its own funding line and is thus able to procure its own systems, whereas the other unified and specified commands depend on the service components to procure or acquire their systems. As a result, the different perspectives of the services and the CINCs immediately create disputes over interoperability and competing priorities.

Under guidelines and public law, requirements are identified by the warfighting CINCs and then codified and acquired or procured by the services, which have the responsibility under United States Code (USC) Title 10 to "equip the forces." Victor DeMarines described the problem plaguing joint C2 as "the difficulty of achieving horizontal integration in a vertically funded world."[19]

Most criticism in the past has charged the services with having perspectives and priorities that do not match those of the CINCs or warfighters. The CINCs argue that

---

[16]Ibid., 43.

[17]Quoted in Chuck Paone, "Office Makes All Pieces of the Puzzle Fit Together," *Hansconian* **44**, 38 (Sept. 22, 2000), 3.

[18]DeMarines, 75.

[19]Ibid., 77.

> Warfighter input (especially that from a joint perspective) can be diluted when individual services are responsible for the articulation of system performance requirements and specifications. The reason is that while the initial specification of requirements may indeed be joint and operationally based, all development projects entail further refinement of specifications as they proceed (this is especially true if a spiral development process is used). A service perspective—rather than a joint one—is thus automatically present as such refinement proceeds. For C4I systems that are primarily of interest to one service, such a perspective will probably enhance the outcome. But if the system is primarily of interest to a joint commander, or if the system is likely to depend on data provided by C4I systems in other services, a service perspective may well detract from (joint) interoperability and/or full functionality.[20]

Such critiques, by focusing on issues related to "turf," no doubt capture an important reason for the friction between services and joint commanders, but in some cases place unfair blame on the service components. Part of the difficulty is that a service often does not know how the proposed system is to be deployed operationally—a problem related to the volatility of the world situation and to ongoing changes in the nature of warfare (section **4.4**). The result is that a service sometimes produces an Operational Requirements Document that does not capture what the system must do or what it must interoperate with. By the time joint commanders review a proposed system, it may be too late to make significant changes.

Viewpoints diverge not only between the services and the CINCs but also among the regional CINCs, who often have different requirements. This is demonstrated on a micro level by the challenges that SOCOM faces in supporting the regional CINCs:

> SOCOM has from its inception placed a very high priority on understanding the needs of the regional CINCs who actually employ the Special Forces that SOCOM trains and equips. This has led to a heavy emphasis on making C2 systems fully interoperable with those of the CINCs, even at the expense of standardization. For example, a special operations unit that moves from the Pacific Command to the European Command may require two full days to modify its organic C2 systems.[21]

Another area of contention is the time frame of interest. Because the CINCs need to focus primarily on fighting today's war, they do not generally look toward future requirements. By contrast, the services continually look ahead in order to plan, program, and budget to replace current force structure. Thus, they are by necessity more visionary. While this difference can cause conflict with a CINC who wants the services to meet a current requirement, it is

---

[20] *Realizing the Potential of C4I*, Chapter Four, 43–44.

[21] DeMarines, 75.

understandable why, in an environment with limited funds, a service may decide not to fund some of today's requirements and instead reserve its budget to meet tomorrow's needs.

4.5.2 Conflicting Priorities for C4I versus Weapons Systems

C2 systems do not yet fit neatly into the DOD's acquisition system, although the DOD is seeking to give them a higher priority (see **Chapter Five**). According to General William F. Kernan, CINC of JFCOM as of September 2000, "Most defense acquisition budget is focused on large-scale systems such as vehicles, ships, and aircraft. But the military's command, control, communications, and computer capabilities are essential to synchronous operations."[22] The NRC report drew similar conclusions: "The organization, procedures, and regulations governing acquisition of military capabilities are oriented largely toward major weapon systems for which the time from concept definition to fielding of the first article of production typically ranges from 10 to 15 years."[23] C4I systems must compete in the service budgets with hardware that the services are obligated to provide under the terms of the National Security Act. "Those rules are built so that DOD spends most of its dollars on ships, tanks, and airplanes; they don't fit command and control systems very well."[24] The NRC report predicts that the military services will face a continuous need to readjust the balance between weapon systems and C4I technology.[25]

The low priority accorded C4I is not new. In 1980, William Odom, former military assistant to the president's assistant for national security affairs, described this environment:

> Who do you think pays for the JCS and the CINCs and the President's command and control—or, to put it colloquially, their telephone bill? The military services. And this creates enormous budgetary and political strain with the Defense Department. If the Air Force has a choice between buying more airplanes or providing a command and control plane for the President, and providing more radios and more ADP [automated data processing] capability for control of the center of the JCS, they prefer the airplanes, not the control. The Army prefers tanks to paying for the

---

[22]William H. McMichael, "Uncertainty, Challenges Await Kernan," *Air Force Times* **61**, 29 (Feb. 12, 2001), 16.

[23]*Realizing the Potential of C4I*, Chapter Four, 15.

[24]Lee Paschall, "C^{3}I and the National Military Command System," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1980* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-80-6, December 1980), 67–86, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/paschal\paschal-i80-6.pdf

[25]*Realizing the Potential of C4I*, Chapter Four, 8.

> President's White House communications system. The Navy has its preferences along the same lines.[26]

Decreases in the DOD budget since the early 1990s require that the department get the most out of limited dollars. Usually, if the DOD must choose between capability and interoperability, capability wins.[27]

4.5.3 Interoperability versus Performance Priorities

According to Victor DeMarines:

> the experience of several decades suggests that the critical decisions will be the engineering trade-offs necessarily made in the course of developing or modernizing any state-of-the-art system. At any given moment in time, the constraints of technology, budget, and schedule always require that some performance objectives be compromised to achieve others…the individual system program offices…tend to assign the highest priority to functionality, the second to interoperability with other systems of the same service, and the third to joint interoperability.[28]

The program manager in charge of acquiring a particular system is graded on three items: cost, schedule, and performance. Cost is considered the fixed variable, which leaves schedule and performance as tradeoffs. Pressures to remain on schedule so as not to drive up costs mean that performance then becomes the tradeoff. One manifestation of the pressures is the importance of reprioritization as a result of tradeoffs between interoperability and security. It can lead to significant reductions in interoperability as the services seek to maintain security and meet schedule and budget commitments.

4.6 Oversight

The DOD does have control over the degree of oversight it exercises—the second area that should be improved if interoperability is to be achieved. After establishing the priorities and codifying them in policy and guidance, the DOD needs to enforce its directives if it is to reach its goals. In 1982, Air Force General Robert T. Marsh, then commander of Air Force Systems Command, said, "I think all [the Secretary of Defense] has to do is saddle up somebody in OSD

---

[26]William Odom, "C^3I and Telecommunications at the Policy Level," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1980*), 12.

[27]*Realizing the Potential of C4I*, Chapter Four, 8.

[28]DeMarines, 74.

and give him the clout to enforce interservice integration.[29] They've tried to do that with the C^{3}I position, but they've just never given it the authority and the responsibility to do it."[30]

Oversight includes making certain that the systems are tested, evaluated, and certified as interoperable. In 1999–2001 the DOD issued directives aimed at codifying the process to ensure that interoperability requirements are included in system specifications and that systems are tested and certified. It will take years to evaluate the impact of this guidance. In the meantime, the DOD needs to deal with persistent problems related to oversight, and, if its initiatives fail, these problems will continue to plague efforts to achieve interoperability. The specific concerns are the different oversight requirements associated with different acquisition categories, ineffective or ignored directives, and the failure of organizations to comply with requirements for interoperability certification.[31]

4.6.1 Level of Information Systems Programs

Different levels of acquisition programs are based on dollar thresholds and importance and receive correspondingly different levels of oversight. The majority—an estimated 80 percent—of information systems are placed in acquisition category 3 (ACAT3), which receives less oversight than the ACAT1s or ACAT2s. The oversight to ensure that interoperability requirements are met for the majority of systems falls to the services, rather than to OSD. "The service acquisition executives must ensure that ACAT2/3 programs meet Joint Interoperability requirements, since the programs (and to a lesser extent ACAT 1C) typically do not get close scrutiny at the OSD level."[32] The remaining 20 percent meet the dollar threshold for category 1 or are important enough for their requirements to be appraised by the Joint Requirements Oversight Council, the Defense Acquisition Board, or the Major Automated Information Systems Review Council. Even review by these bodies does not guarantee a careful assessment, because they perform review and oversight functions for many programs. Thus, the attention that they can give to any specific program is limited.[33]

---

[29]In this context, "interservice integration" meant interoperability of communications equipment "owned" by different services.

[30]Robert T. Marsh, "Air Force C^{3}I Systems," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1982* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-88-1, May 1988), 103, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/marsh\marsh-i88-1.pdf

[31]For a detailed discussion of the current oversight process as it relates to C4ISR systems and suggestions for several useful modifications to the current system, see Walter P. Fairbanks, *Information Superiority: What Is It? How to Achieve It?* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-99-4, June 1999), 50–57, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/fairban\fairban-p99-4.pdf

[32]Robert M. Nutwell, prepared speech on "Achieving Joint Information Interoperability," Version 1, April 4, 2000, 14–15.

[33]*Realizing the Potential of C4I*, Chapter Four, 54.

4.6.2 Enforcement of Directives

Oversight also needs to be improved to promote interoperability in the enforcement of directives. A 1998 report by the DOD's inspector general notes that "directives intended to assure jointness and interoperability of C4I systems have proven relatively ineffective because program managers and the services have few institutional incentives to comply with them, and few penalties accrue to C4I programs that are not interoperable."[34] As mentioned in section **4.3.2,** few commercial products initially met the standards established for the JTA, and additions only complicated the standard for system interfaces. Despite a directive by the ASD C3I that made the JTA mandatory for all C4I systems, the inspector general's report found noncompliance in the plans of many C4I programs. If that occurs for a program with written plans, one can only assume that some others with compliance written into their plans will not comply.[35]

The DOD's offices responsible for oversight argue that they lack the authority to enforce compliance because they do not control the money that is the "carrot" or "stick" for the services and agencies. The NRC report, however, placed the greatest blame on the overall process:

> While certain C4I oversight offices within DOD do have the ability to withhold budget authority from the services for C4I programs that are not paying sufficient attention to C4I interoperability, they do not in general have budgets of their own to spend on efforts to promote interoperability. Stopping programs that do not comply with requirements for interoperability requires identifying them in the first place, and then investing time and political capital—a highly inefficient process.[36]

As a result, "the behavior of program directors and managers has evolved little—nor has that of an oversight process established to ensure that every acquisition of significance satisfies the traditional acquisition regulations."[37]

4.6.3 Certification of Information Systems

The services and defense agencies have tended to ignore the standing requirements for systems to be certified by the JITC. In 2000, the JITC commander stated that the services or agencies simply do not bring their systems to the JITC for testing and certification.[38]

---

[34]Ibid., 12.

[35]Ibid.

[36]*Realizing the Potential of C4I*, Chapter Four, 12.

[37]Ibid., 37.

[38]Ben Osler (Colonel, USAF), Commander, Joint Interoperability Test Center, in telephone interview with the author, October 2000.

A 1998 GAO report revealed that a significant number of C4I systems were not submitted for testing, so that testing covered none of the systems developed under the C2 initiatives program or under the advanced concept technology demonstration program in the three years since 1995. The GAO also found that there was no consistency with regard to recertifying modified systems. Lastly, the GAO charged that the JITC was not advising the services of interoperability problems identified in exercises, even when the problems, shortfalls, or failures could have resulted in loss of equipment, supplies, or even lives.[39]

In 1998 the DOD issued directives requiring JITC certification before a system is allowed to go into production. It remains to be seen whether the services will comply with them. The JITC is a fee-for-service organization, which means that the services must pay to have their systems certified. This cost may help explain the reluctance. The track record and the lack of enforcement of the requirements suggest that compliance may well be spotty or slow to come.

4.7 More Frequent and Realistic Training and Exercises

A final factor over which the DOD has control is training. In the Navy's lessons learned, Vice Admiral Stanley R. Arthur, commander of Navy Central during Desert Storm, emphasized the need to focus on interoperability: "when deployed, joint and multinational operations/ exercises should focus on interoperability issues—comms [communications], tactics, limitations."[40]

Training provides the opportunity not only to train personnel, but also to identify equipment and system interoperability shortfalls so they can be fixed. More important, training needs to provide realistic assessments of both personnel and equipment so that remedial or corrective actions can be taken to overcome deficiencies. The goals of training can be accomplished only if equipment and people are exercised frequently and in a realistic environment.

This difficulty is not new. In the course of a discussion during the 1981 C3I seminar at Harvard University, Robert R. Everett, president of The MITRE Corporation from 1969–1986, noted:

> Now as it turns out, the German and the French PTTs [postal, telephone, and telegraph agencies] will work together; the French and the Germans do talk to each other, and that has been true ever since the early days. Therefore, in the course of evolution, it's worked. But if they had never

---

[39]U.S. GAO, *Joint Military Operations: Weaknesses in DOD's Process for Certifying C4I Systems' Interoperability* (Washington D.C.: U.S. GAO, Report No. NSIAD-98-73, 1998), cited in *Realizing the Potential of C4I*, Appendix B, 22–23.

[40]U.S. Dept. of the Navy, "Lessons Learned and Summary," in *U.S. Navy in Desert Shield/Desert Storm*, *Quick Look—First Impressions Report* (Washington, D.C.: U.S. Dept of the Navy, Naval Historical Center, March 22, 1991), 1, [On-line]. URL: http://www.history.navy.mil/wars/dstorm/ds6.htm (Accessed on Jan. 2, 2001.)

> talked to each other and a time comes, at two o'clock in the morning, when they will need to talk together, rest assured they won't be able to. This is the situation in our military. People say, 'It's just absurd that the Army and the Navy can't talk to each other. We'll legislate it: Everybody shall buy the same radios; or, we'll make them get together in one room and design the communications center.' Those things don't work. The only way you're going to get them to work together is to make them work together, make them work joint exercises, and when they can't work together and the thing fails, you sneer at them and they have to go out and fix it. If you don't do that, they won't ever fix it.[41]

Everett hit the nail on the head: the key to enabling people and systems to work together lies in joint training. Training needs to be conducted frequently to promote maximum readiness. As of 2001 most training is conducted only at the unit levels of individual services, not jointly. By statute, the services also have the responsibility for training the forces, so a large component of training is unit exercise. Because unit training usually involves other units and systems from the same service, it is more likely to identify and fix interoperability shortfalls within the services so as to maximize intraservice operations than to pinpoint interservice incompatibilities. By contrast, joint exercises and training are relatively infrequent, and each exercise involves interactions among different sets of equipment, depending on the units that happen to train together. Even when particular impediments are identified, any pressure to fix problems arising in a joint context is far less immediate—because the unit will not exercise with that particular unit again for a long time (if ever)—than the pressure to fix problems arising in same-service unit exercises, which are more frequent and subject to greater scrutiny. Joint exercises therefore lack local incentives, and many obstacles to interoperability may remain hidden because the systems are not exercised often or thoroughly enough.[42]

Equally important is the frequency of training and exercises. More frequent exercises are required to evaluate and enhance the readiness of personnel to perform their tasks in joint operations. Again, because of infrequent opportunities to participate in joint exercises, individual service members are not exposed to realistic conditions or trained as they are expected to fight. Take, for instance, Cobra Gold, conducted annually in Thailand. Because the Joint Task Force (JTF) headquarters rotates each year between the U.S. Army First Corps and the U.S. Marines Third Marine Expeditionary Force, the Air Force unit that provides communications support for the Air Operations Center gets to exercise with each of the JTF headquarters only biannually. Given the rotation of personnel, a significant percentage of people will be deploying to the area for the first time and will therefore receive insufficient training to maintain optimal skills.

---

[41]Robert R. Everett, quoted in *C³I: Issues of Command and Control*, edited by Thomas P. Coakley (Washington, D.C.: National Defense University Press, 1991), 185.

[42]*Realizing the Potential of C4I*, Chapter Four, 11.

Joint training needs to be not only frequent but also realistic. Exercises are usually designed to maximize operational objectives but do not realistically test deployment or employment of communications systems. The communications systems are set up and networks are established well before the operational forces arrive, and during the exercises communications outages or problems are simulated so as not to risk a real outage, which might jeopardize operational goals.

Communications systems and procedures that are prepared in advance naturally work better than communications systems that must be set up in an actual combat situation. This was one of the lessons learned stressed by Admiral Wesley L. McDonald, CINC of ACOM, in testimony before congressional hearings on the Grenada operation:

> We do conduct communications exercises in the Navy, but in these exercises, we give our communications about 12 months' preparation. Therefore, it should not be surprising that when the exercises start, communications work…. Our failure in preparatory exercises to uncover and anticipate problems similar to those we faced in Grenada may have been because our exercises are over prepared. Given enough time, anyone can make communications work. Unfortunately, in a crisis situation—a "come-as-you-are" situation—they do not work.[43]

Part of the difficulty may be an erroneous conclusion drawn from Desert Storm: that realistic training for deploying and employing communications is not necessary, because coalition forces had six months to set up and establish communications prior to hostilities. In the usual manner of always fighting the last war, and despite the need for realistic training that was emphasized twenty years ago, the norm during exercises is still for the communications personnel and equipment to deploy early and establish communications ahead of the arrival of the operators. In the Cobra Gold exercises, the people and equipment ordinarily arrive in Thailand two weeks to a month prior to the start of the exercise—and even so problems still occur when the operators arrive. Such advance preparation fails to reproduce realistically the concept of rapid deployment and the philosophy of "come as you are" and therefore undermines the purpose of the exercises.

Simulations also play a central part in determining realism. In many cases, duplicate systems are built to simulate real-world systems and to keep exercise communications separate from real-world communications. Often incapable of directly duplicating operational C4I systems (such as databases, interfaces, traffic loads, etc.), the surrogate systems created to carry out the exercises are not sufficiently similar to the actual systems to provide adequate training or to

---

[43]Stephen Anno and William E. Einspahr, "The Grenada Invasion," in *Command and Control Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid* (Maxwell Air Force Base, Ala.: Air University Press, Air War College Research Report, No. AU-AWC-88-043) [extract reprinted from the original research report by the U.S. Naval War College Operations Department, NWC 2082], 43, [On-line]. URL: http://www.fas.org/man/dod-101/ops/urgent_fury.htm (Accessed on Feb. 5, 2001.)

identify shortcomings in interoperability.[44] For example, scenarios of communications failure simulated to maximize operational training, the systems are not actually taken off line, which would realistically demonstrate the lack of capability. Simulations thus deny realistic training to both the operational and communications personnel.

In her book on coalition warfare, Martha Maurer paid particular attention to the issue of simulations, pointing out that many exercises have a primary operational orientation where unknowns or less important concerns, such as C3 availability, are simply assumed not to exist. Maurer emphasized that the services need to test C2 systems as if in war or in absolute reality; otherwise, the systems cannot be evaluated effectively.[45] The challenge is twofold: the exercises need to use the systems that will be employed in combat, and the scenarios designed to exercise communications outages or degradations need actually to take the systems off line instead of merely simulating their unavailability. Without such realistic simulations, neither operational nor communications personnel will be effectively evaluated, and the opportunity to improve operations or fix problems will be missed.

Although all of the experts cited here stress the dichotomy between what exercises are officially meant to achieve and what the participants actually seek to achieve, exercises, however flawed, have contributed to operational successes. Take the U.S. Navy's experience in Desert Shield/Desert Storm and the practical effectiveness of SOCOM. The Navy attributes much of its success in the Persian Gulf war to appropriate exercises, in which years of close cooperation and coordination with the navies of NATO allies and other coalition partners in regular bi- and multilateral exercises and during the Iran–Iraq war [1980–88] laid a strong foundation of interoperability and common procedures.[46]

The DOD never wishes to place people unnecessarily in harm's way, but ideally it should test C2 systems in real-world settings such as those experienced by SOCOM. SOCOM attributes much of its successes to experience, noting that its forces have frequently been involved in real operations against real enemies. Its C2 systems are frequently tested in operational conditions, in which any failures of C2 interoperability will become obvious and will be remedied immediately.[47] This opportunity does not exist for the rest of the military, so the only way to train and evaluate personnel and systems is through highly realistic exercises and training.

In summary, the DOD needs to expand and improve its efforts to make exercises and training realistic and timely, and to increase the frequency of training to ensure that people are trained and equipment maintained at peak performance. More realistic exercises mean that

---

[44]*Realizing the Potential of C4I*, Chapter Four, 63.

[45]Maurer, *Coalition Command and Control*, 105.

[46]*U.S. Navy in Desert Shield/Desert Storm*, 1.

[47]DeMarines, 75.

equipment and personnel need to be deployed and employed during exercises as might be expected in actual combat, not weeks or a month ahead of the arrival of the operators. Furthermore, the DOD should minimize the use of simulations and, when these are unavoidable, design them so that they mirror real-world operations as closely as possible in order to evaluate personnel and identify equipment problems that need to be remedied.

Chapter Five

Mitigating Initiatives

There are many Joint Interoperability initiatives underway addressing several fronts: policy, requirements, acquisition, resources, process, and procedure. Coordination of these varied activities is difficult at best. Cost is high and the actual result of these efforts is yet to be determined.[1]

The DOD has instituted several changes to policy and guidance, organizational roles, and the acquisition process that are aimed at mitigating the effect of the factors addressed in **Chapter Four** and at promoting interoperability. It will take years to implement the DOD's initiatives and even longer to determine their overall success, but they will definitely affect future interoperability. If these initiatives do succeed, the prospects for interservice interoperability almost certainly will improve.

5.1 New Policy and Guidance

Three related policy and guidance documents, updated and implemented in 1999–2001, made interoperability a priority and hold the potential for improving interoperability among the services. These are the DOD Instructions (DODIs) 5000 series, which governs the acquisition process, and two CJCSIs, the first mandating procedures for generating requirements, the other addressing interoperability and support to national security systems and information technology systems.

The earliest of these documents, signed into effect on August 10, 1999, is CJCSI 3170.01A, *Requirements Generation System*, which sets policy for the CINCs, services, and agencies regarding how requirements are identified and systems procured to meet the requirements. This document contains three significant changes from previous policy related to interoperability. Two of them—time-phased requirements in support of evolutionary acquisition and the roles of JFCOM—are discussed under the headings of organizational changes (section **5.2**) and acquisition initiatives (section **5.3**). The third change involves key performance parameters (KPPs).

CJCSI 3170.01A established a first by mandating that interoperability KPPs be included in requirements documents and mission-need statements—the two critical documents in the acquisition system—for major automated information system acquisition programs.[2] Including

---

[1]Paul D. Szaboados, Office of the Deputy Assistant Secretary of Defense for C3ISR, and Support/Program, Analysis, and Integration, issue paper, subject: *Joint Information Interoperability Initiatives 2000* [no date].

[2] CJCSI 3170.01A, *Requirements Generation System*, (Washington, D.C.: Office of the CJCS, Aug. 10, 1999), 3.

interoperability in the KPPs means that acquisition programs must meet systems interoperability requirements by the end of each phase of the acquisition cycle (e.g., concept exploration, component advanced development, system development and demonstration, production and development) prior to advancing to the next phase.

CJCSI 6212.01B, signed into policy on May 8, 2000, builds on the methodology presented in 3170.01A to help create interoperability. This document describes a procedure for developing interoperability KPPs and links the KPPs to a set of information exchange requirements (IERs),[3] defined as information exchanges among CINC, service, agency, and coalition systems. In lay terms, an IER "identifies who exchanges what information with whom, why the information is necessary, and how the information must occur."[4] IERs represent a breakthrough, because previously performance was tied to a vague standard such as the JTA or DII/COE, but the CJCSI defines it in relation to the systems from within the service and among other services with which the systems must operate. By establishing minimum threshold criteria and objective (desired) criteria for accomplishment of KPPs before an acquisition program can proceed to the next milestone, CJCSI 6212.01B makes interoperability a "showstopper" for the first time. The threshold criteria, which are the minimum IERs a system must satisfy, are typically defined as all or 100 percent of the critical (minimum essential) IERs, with the objective criteria being the accomplishment of all the remaining IERs.

Lastly, the CJCSI puts in place a mechanism for the Joint Staff's J-6[5] validation process that mandates the J-6 review of requirements and certification documents to ensure that all systems meet the interoperability KPPs. This J-6 validation is intended to provide oversight throughout the entire life cycle of warfighter interoperability requirements. Validation affirms that the interoperability KPPs derived from the set of IERs approved in the requirements documents and C4I support plan were adequately tested and testing the results certified.[6]

The DODIs were signed into effect on January 4, 2001. DODI 5000-2 reiterates that all information technology acquisition programs developed for U.S. forces must be for joint, combined, and coalition use or, in words commonly used by Pentagon action officers, must be "born joint."[7] It strengthens the prospects for achieving interoperability by expanding the policy established by the two CJCSIs discussed in this section to all acquisition categories, so that "The

---

[3]Joint Staff/J-6I, "CJCSI 3170.01A 'Requirements Generation System' and CJCSI 6212.01B 'Interoperability and Supportability of National Security Systems, and Information Technology Systems,'" briefing by Commander Mark Genung, USN, Jan. 16, 2001, slide 8.

[4]Ibid., slide 7.

[5]The Joint Staff J-6 is the director of communications for the CJCS Joint Staff.

[6]CJCSI 6212.01B, *Interoperability and Supportability of National Security Systems and Information Technology Systems* (Washington, D.C.: Office of the CJCS, May 8, 2000), 4.

[7]DODI 5000.2, *Operation of the Defense Acquisition System (Including Change 1)* (Washington, D.C.: OSD, Jan. 4, 2001), 11.

Chairman of the Joint Chiefs of Staff shall establish procedures for the development, coordination, review, and validation of interoperability and supportability of IT (including NSS [National Security Systems]) acquisition programs, regardless of acquisition category."[8] This requirement is a major change aimed at overcoming the inadequate oversight associated with those lower category programs (see section **4.6.1**).

5.2 Organizational Changes

As noted in section **3.2.3**, the path to organizational evolution and responsibility began in 1993, when ACOM was assigned responsibility for training and providing forces based in the continental United States (CONUS) to support the needs and operations of the regional CINCs. When ACOM was rechartered as JFCOM in October 1998, it was given broad responsibilities for supporting joint operations, which include being the joint force integrator. The provisions of the UCP, which assigns responsibilities to the CINCs, gave JFCOM a mandate to promote jointness and chartered its involvement in the joint requirements process.[9] CJCSI 3170.01A codified the command's role for interoperability and, in another first, assigned responsibility to act as the advocate for interoperability: "USCINCACOM will serve as the Chairman's advocate for joint warfighting interoperability. USACOM will provide the warfighter perspective during the development of joint operational concepts to ensure that joint forces have interoperable systems."[10] As a result, JFCOM has the opportunity to participate at every level of decision-making—from the integration process team, to CINC involvement in the requirements oversight process, to the Defense Acquisition Board that oversees and approves the acquisition of major weapons and automated information systems.[11]

> Accordingly, the command has begun to advocate jointness and interoperability in generating requirements which provide opportunities to influence the development and approval of all mission needs statements regardless of acquisition category or origination source and the staffing of service-generated operational requirements that is critical because these documents define program performance parameters for improving interoperability.[12]

Since inheriting its new mission, JFCOM has made interoperability a primary focus. A February 2001 interview with the CINC for JFCOM, General William F. Kernan, highlighted the

---

[8]Ibid.

[9]Victor A. DeMarines, "Exploiting the Internet Revolution," in *Keeping the Edge: Managing Defense for the Future*, edited by Ashton B. Carter and John P. White (Cambridge, Mass.: MIT Press, 2001), 79.

[10]CJCSI 3170.01A, B-7.

[11]Harold W. Gehman, Jr., "Progress Report on Joint Experimentation, *Joint Forces Quarterly* **25** (Summer 2000), 82 [On-line]. URL: http://www.dtic.mil/doctrine/jel/jfq_pubs/1325.pdf (Accessed on March 6, 2001.)

[12]Ibid.

CINC's pivotal role in ensuring interoperability: "If a system does not fill the interoperability requirements…Kernan can give it the boot."[13] Although this assessment of Kernan's authority may be debated, the designation of an operational CINC to act as the advocate for interoperability and the involvement of JFCOM in the requirements and acquisition processes for all automated information systems both carry tremendous potential for promoting interoperability.

JFCOM also plays a leading role in training:

> With calls for improved interoperability among the services, the Joint Chiefs recommended that ACOM be assigned responsibility for joint training and integration. Changes in the Unified Command Plan directed that then ACOM assume peacetime control over U.S. Army Forces Command and Air Combat Command. Today, JFCOM is the provider, trainer, and integrator of joint forces.[14]

Putting a CINC in charge of training and integrating joint forces and then assigning control of the CONUS forces to that CINC provides the leverage for increased joint training.

The October 1998 UCP also assigned ACOM responsibility for the DOD's Joint Experimentation Program, which is aimed at exploring and validating future joint operations and concepts that will drive changes to doctrine, organization, training, and education, materiel, leadership, and people (known collectively as DOTMLP). With this responsibility the command added a Joint Experimentation Directorate, J-9, in October 1998, which laid the foundations for "working with the services, unified commands, defense agencies, industry, and academe on exploring new concepts."[15]

The experimentation program does not rely solely on simulation, but combines simulation with real operational exercises. "Some good things can be done by computer-driven modeling and simulation, but sooner or later, we must try new operational measures in the air, at sea, and on the ground."[16] For example, from fleet exercises in the 1930s, which defined carrier warfare, to the Army's famous Louisiana Maneuvers of 1941, which developed air-ground operations for combined arms, the U.S. experimentation program relied on live war games.[17] JFCOM hopes to obtain similar results from exercises such as Millennium Challenge 2002, which it designed to

---

[13]William H. McMichael, "Uncertainty, Challenges Await Kernan," *Air Force Times* **61**, 29 (Feb. 12, 2001), 16.

[14]Gehman, 78.

[15]Ibid.

[16] U.S. Joint Forces Command, Mission Statement, subject: USJFCOM Command Mission, 2, [On-line]. URL: http://137.246.33.101/cmdmission1.htm (Accessed on March 3, 2001.)

[17]Ibid.

exercise service operational concepts and examine and identify strengths and weaknesses in the interoperability and the integration of service warfighting concepts into a joint environment.[18]

5.3 New Acquisition Process

Although it cannot control the rate of change in technology (see section **4.3**), the DOD has modified its traditional acquisition strategy in an effort to minimize the impact of rapid change. As the NRC report acknowledged, "The realization that the rate of change in technology as well as in operational requirements (especially in C4I) is not matched to the typical multiyear cycle time for traditional system acquisition has led to the concept of evolutionary acquisition, also known as 'spiral development.'"[19] Given a validated requirement and an approved architectural framework for future development, evolutionary acquisition allows more rapid deployment of systems and provides a process for incremental upgrading of fielded systems. It enables program managers to execute the requirements, definition, testing, and fielding steps of traditional acquisitions over much shorter cycle times than previously for each phase of system deployment. Evolutionary acquisition permits the addition of new capabilities to a system as the underlying technologies evolve without this being viewed as "requirements creep."

One of the three main thrusts of CJCSI 3170.01A (section **5.1**) is related to the evolutionary acquisition approach. The document codifies time-phased requirements in support of an approach aimed at a streamlined acquisition strategy that fields a core capability with a modular open structure and provides for future incremental upgrades in capability. The instruction states that "Automated Information Systems are prime candidates for evolutionary acquisition,"[20] which will help cope with and take advantage of rapidly changing and developing technology.

In its discussion of evolutionary acquisition, the NRC report strongly recommended that virtually all C4I acquisitions aim at the "80 percent solution," which enables the program to accommodate technical improvements that will occur over the development period and involves the end user in all phases of the acquisition cycle. This approach acknowledges the reality that it is undesirable, even impossible, to specify all C4I system requirements fully, given the time lag between the approval and deployment of any major military system. A 100 percent solution, which would mandate not only the goal of the new system but also every item of equipment used to achieve it, would mean a system that would be out of date by the time it was fielded. By

---

[18]U.S. Joint Forces Command, "Background," in Instructions for Joint Initiative Submission and Review Process for Millennium Challenge 2002, 1, [On-line]. URL: http://137.247.242.50/Key%20Reports/Instructions%20v4%20-%20to%20CoS.doc (Accessed on March 3, 2001.)

[19]NRC, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy Press, December 1999), Chapter Four, 16, [On-line]. URL: http://books.nap.edu/books/0309064856/html/64.html (Accessed on Nov. 6, 2000.)

[20]CJCSI 3170.01A, 3, E-2.

contrast, an 80 percent solution identifies the system objectives and provides the overall framework while allowing flexibility in the actual equipment used to achieve target functionality. This incremental approach allows program managers to gain experience with technological change that will become invaluable for specifying and building the target functionality. It also allows for changes in doctrine and tactics that respond to the evolving capabilities of the new system.[21]

Military personnel often cite the Global Command and Control System (GCCS) as one of a very few examples of successful acquisition of a major C4I system, and the NRC report echoed this assessment. The GCCS acquisition process reflected the 80 percent rule and enabled GCCS to replace the outdated Worldwide Military Command and Control System in approximately two years (GCCS was activated on August 30, 1996). Because the GCCS was not designated a "major" acquisition program, it was not subject to many burdensome reviews or test and evaluation phases. Most important, the acquisition process did not require formally validated specifications at each stage, but, instead, featured short phases and milestones and responded to emerging requirements by initiating repeated evolutionary cycles.[22] However, there is a downside to rapid deployment and the 80 percent rule in the acquisition process. For example, JFCOM has identified over 100 high-priority remedial actions that need to be taken to make GCCS operationally suitable.

[21]*Realizing the Potential of C4I*, Chapter Four, 16–18.

[22]Ibid.

Chapter Six

Interoperability: Is It Really Achievable?

6.1 Recapitulation

Lessons learned from two decades of operations reveal continuing problems with interoperability among U.S. forces and between U.S. forces and allied, multinational, and coalition forces. They acknowledge and emphasize the essential role of interoperability in ensuring the most efficient and effective future joint operations. In addition to recognizing the obvious indicators—that joint operations require joint C2, which in turn requires interoperability between the systems of the different services—the DOD has sought to respond to shortfalls in interoperability and their impact on future operations, to insufficient attention paid to these shortfalls by senior leadership, and to the emphasis that warfighters (CINCs) place on interoperability. Given the influence that the Goldwater–Nichols Act of 1986 bestowed on the CINCs, the DOD's naming of an operational CINC as the advocate for interoperability becomes significant.

Despite the recognition of its importance and the enormous efforts exerted toward achieving it, however, interoperability continues to elude the DOD. A combination of complex factors continues to haunt U.S. joint operations, among them, shrinking budgets, rapidly changing technology, the changing nature of operations, the lack of priority accorded to interoperability, lack of oversight, and unrealistic and infrequent joint training.

The good news is that the DOD continues to work aggressively to mitigate the effects of the factors that make achieving interoperability difficult. Since 1999, a tremendous effort has resulted in the promulgation of new visions mandating interoperability, of policy that codifies requirements for interoperability KPPs, and of certification procedures for "all" automated information systems acquisition. Organizational changes in the DOD also promise to improve the prospects of achieving interoperability. By designating JFCOM as the joint force "integrator" and "interoperability advocate" and assigning to it responsibilities for joint training and for reviewing and providing input to all systems acquisitions, the DOD has charged a single operational command with improving interoperability through training and with assuring interoperability of new systems.

6.2 What Does the Future Hold?

Will the DOD's efforts to achieve interoperability succeed, or even make a significant difference? No one can predict with certainty. This report makes no specific recommendations, but presents the following thoughts for consideration.

Although the DOD has no control over such factors as the pace of technological change or the occurrence of international crises, there are steps it may take to mitigate the associated circumstances. For example:

- Because future operations will probably continue to involve either joint U.S. forces or more likely, joint U.S. forces working with allied, multinational, and coalition forces, new systems will need to be born joint, and modifications to existing systems will need to enable joint interoperability.
- Because defense budgets will probably stay essentially the same as in 2002 (the date of this report), with the most optimistic scenario being a slight increase in real dollars, tradeoffs will need to be made intelligently in coordination with the warfighters or operators and interoperability will need to be included in initial acquisitions to prevent expensive, often unbudgeted modifications after fielding.
- Because technology will continue to change rapidly (prompting the DOD to maintain its approach of seeking creative acquisition strategies, such as the evolutionary or "spiral down" approach, to take advantage of the latest technical innovations), the DOD will also need to continue its efforts to define standards to ensure interoperability between the newest technical systems and legacy systems.

By contrast, the DOD does control its own destiny in several areas that affect interoperability. If the DOD were to fail to provide sufficient and effective oversight, its recent efforts to update and promulgate visions, policy, and guidance will have been for naught. The DOD as a whole and the services individually need to make certain that acquisition procedures accord interoperability the priority commensurate with its importance so that interoperability can prevail through tradeoffs in capability and functionality. The DOD and the services also have the capability to make joint exercises and training more frequent and realistic to ensure that the forces are ready for rapid "come-as-you-are" deployments. Only through such training can the U.S. military identify shortfalls in doctrine, tactics, procedures, and equipment performance so these can be corrected. The DOD needs to tear down the barrier between technicians and operators so that those responsible for the information systems understand the operational setting in which the systems will be used. Finally, as military and civilian leaders in the DOD agree, the military needs to provide greater incentives to recruit and retain technically and operationally proficient people.

Perhaps the military can acknowledge and adopt what the Navy identified as its final lesson learned from the Persian Gulf war: "The naval forces and capabilities put to the test in Desert Shield/Desert Storm were not achieved by decisions made in the last few years…[they] were products of decisions made throughout the 1980s. So a final lesson might well be that the decisions we make today do have important ramifications for the future."[1] Although complete

[1]U.S. Dept. of the Navy, "Lessons Learned and Summary," in *U.S. Navy in Desert Shield/Desert Storm*, *Quick Look—First Impressions Report* (Washington, D.C.: U.S. Dept. of the Navy, Naval Historical Center, March 22, 1991), [On-line]. URL: http://www.history.navy.mil/wars/dstorm/ds6.htm (Accessed on Jan. 2, 2001.)

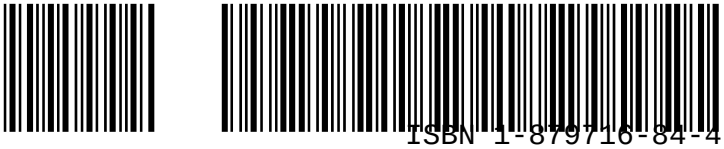
interoperability will almost certainly never be achieved, the DOD's decisions at the beginning of the twenty-first century regarding interoperability may well hold the answer to the question, "Is interoperability achievable?"

Acronyms

ACAT	acquisition category
ACOM	U.S. Atlantic Command
ASD	assistant secretary of defense
ATO	air tasking order
C2	command and control
C3	command, control, and communications
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CENTCOM	U.S. Central Command
CINC	commander in chief
CIO	chief information officer
CJCS	chairman, Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COTS	commercial off-the-shelf
DII/COE	Defense Information Infrastructure/Common Operating Environment
DOD	Department of Defense
DODI	Department of Defense Instruction
GAO	U.S. General Accounting Office
GCCS	Global Command and Control System
GTN	Global Transportation Network
IDA	Institute for Defense Analyses
IER	information exchange requirement
IT	information technology
JCS	Joint Chiefs of Staff
JFCOM	U.S. Joint Forces Command
JITC	Joint Interoperability Test Command
JOPES	Joint Operations and Planning System
JTA	Joint Technical Architecture
JTF	joint task force
JTIDS	Joint Tactical Information Distribution System
KPP	key performance parameter

NATO	North Atlantic Treaty Organization
NRC	National Research Council
OSD	Office of the Secretary of Defense
QDR	Quadrennial Defense Review
SIAP	single integrated air picture
SOCOM	U.S. Special Operations Command
STU	secure telephone unit
TADIL	Tactical Digital Information Link
TRI-TAC	tri-service tactical
UCP	Unified Command Plan
USAF	U.S. Air Force


PPFAUGHN


ISBN 1-879716-84-4