USAWC STRATEGY RESEARCH PROJECT

JOINT C4I INTEROPERABILITY – A LOOK AT THE PROCESS FOR ARMY TRANSFORMATION

by

LTC Robert L. Bethea, Jr.
U.S. Army

Mr. William Waddell
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
07-04-2003		xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE
Joint C4I Interoperability-A Look at the Process for Army Transformation
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Bethea, Robert L. ; Author

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Army War College
Carlisle Barracks
Carlisle, PA17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Same as Report (SAR)	37	Rife, Dave RifeD@awc.carlisle.army.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN

ABSTRACT

AUTHOR: LTC Robert L. Bethea, Jr.

TITLE: JOINT C4I INTEROPERABILITY – A LOOK AT THE PROCESS FOR ARMY TRANSFORMATION

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 37 CLASSIFICATION: Unclassified

Network Centric Warfare (NCW) is truly the embodiment of an information age transformation for the Department of Defense (DoD). It will involve new ways of thinking about how we accomplish our mission. It will also require new ways of operating that have not been conceived and employs technologies yet to be invented. Joint integration and joint interoperability will be absolutely required to effectively command and control the battle space of the future. The purpose of this strategic project report is to examine the DoD processes and policies that are in place to ensure joint compliancy for Army command, control, communications, computers and intelligence (C4I) equipment as we move towards DoD and Army transformation.

TABLE OF CONTENTS

PREFACE

There are many people that I would like to thank for their assistance and support during my research for this project. First, I would like to provide a special thanks to my Project Advisor Mr. William Waddell for his direction and advise while helping to guide me through the completion of this research project. Most of all I want to thank him for his patience and understanding. I would also like to thank my wonder children Karina and Kyle Bethea for understanding and allowing me to work on this project while balancing the competing opportunities provided by the United States Army War College experience. Finally, I want to thank my wife, LTC Mearen C. Bethea for her patience, encouragement and unwavering support from long distance while commanding a battalion in Colorado Springs, Colorado.

JOINT C4I INTEROPERABILITY – A LOOK AT THE PROCESS FOR ARMY TRANSFORMATION

Our military is increasingly becoming dependent on information dominance as the key to victory in the conduct of future operations. Terms like network centric operations reflect the increasing demand for interoperability between our services and coalition partners for military operations in the 21st century. The concept of interoperability is not new to warfighters. History provides more than enough evidence to demonstrate how inadequate interoperability can cause major problems, and significantly reduce military effectiveness. A report by the Secretary of Defense noted "from Grenada in 1983 to Operation Desert Storm in 1991, joint operations have been hindered by the inability of forces to share critical information at the rate and at the locations demanded by modern warfare"[1].

Interoperability between Command, Control, Communications, Computers and Intelligence (C4I) systems is a key enabler of the overarching operational goal of force integration. It is the fusing of the services and coalition partners into a unified military force that achieves high military effectiveness, while exploiting and coordinating individual force capabilities. Achievement of a high level of interoperability requires a commensurate level of effort and resource prioritization throughout the Department of Defense (DoD). Today, the DoD is only at the beginning of refining, and even establishing the processes, procedures and organizations to respond to future needs for C4I interoperability. As the Army moves towards the development of the Future Combat System (FCS) during its transformation, interoperability of C4I systems will be critical to successful operations.

Shortfalls in the interoperability among U.S. forces were first publicized by the press at the time of the Grenada invasion, and became the catalysts for legislation and change in defense policy, guidance, and procedures aimed at attempting 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 DoD.

According to a memorandum issued in December 2000 by the Undersecretary of Defense (USD) for Acquisition, Technology, and Logistics; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASDC3I); the 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 Combatant Commanders of

> the Unified Commands have frequently raised interoperability issues via the Joint Staff's Joint Warfighting Capability Assessment (JWCA) process, the CINC Interoperability Program Offices (CIPOs), and other fora. [2]

This paper presents a short account of some of the major issues and concerns associated with achieving interoperability. It will also site historical examples of interoperability challenges experienced by our military while conducting operations. This paper will attempt to define interoperability and clarify why it is so important to our military as we transform to meet the needs for operations in the 21st century. This paper will mainly focus on interoperability as it relates to C4I systems. Additionally, this paper will discuss why achieving interoperability is a difficult process for the military and examine the DoD policies and processes aimed at meeting the interoperability challenge.

The interoperability umbrella covers a wide and varying array of complex issues. To those within our military services, and perhaps to those outside of the military, it seems incredible that problems with interoperability persisted in Kosovo operations after all the effort and money spent in the fifteen years since Grenada. How did these problems evolve and why are Combatant Commanders 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 C4I equipment when it entered the war. The government had to purchase the majority of the C4I systems at the same time, and acquired the same equipment for all services—whether it was ultimately fielded on ships, tanks, or airplanes. This equipment of that era, at least systematically had achieved a reasonable level of interoperability by default.[3]

In the fifty-plus years since World War II, 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 even if the government allocated the money to do it. The funding required to facilitate such as effort just was not practical. Instead, each service procured individual equipment and systems that optimally supported its own activities at particular times. This approach resulted in different generations of equipment that did not interoperate with the material and systems of the other services. This approach may have improved performance at a time when the services operated more or less independently, without joint consideration. With the increase in technology and the advent of joint and combined operations, shortcomings in joint interoperability became all too obvious.

When considering joint interoperability issues there are many factors that hamper the achievement of interoperability. Some of 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, control, communications and computers (C4) and weapon systems; and the ever-changing nature of joint and multinational operations. The human factor and leader education regarding change can also factor into the challenge for interoperability.

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. The interoperability concerns are real and the problem does not go unrecognized. Despite the tremendous planning and expenditure of funds to ensure interoperability, major interoperability problems continue to plague commanders and staffs at all levels of military operations. Joint Vision 2020,[4] published in June 2000, mandates interoperability. The Unified and Specified Combatant Commanders, the four service chiefs and members of Congress all champion its importance.

SHORT HISTORY OF INTEROPERABILITY OVER THE PAST TWO DECADES

A look at the U.S. joint operations in the 1980s and 1990s reveals the importance of interoperability. Although the operations in Grenada drew attention to the inadequacies of interoperability, interoperability was already an important goal even before the invasion. In 1982, Hillman Dickerson, then director of Command, Control and Communications (C3) systems for the Joint Chief of Staff, listed “improved 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.”[5] Our military could not have known that his statement would be validated in less than one year with military operations in the country of Grenada.

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 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 preventing recurring interoperability in the future have never been

confirmed in the unclassified official literature. However there are some unclassified documented lessons learned that acknowledge the problems.[6]

> The final challenge to invading forces was a lack of a fully integrated, interoperable communications system…. Communications was to have been the glue that would tie together the operations 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 communications was prevented, except through offshore relays 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 Ft Bragg, N.C., to obtain C-130 gunship support for his unit which was under fire…. Commenting overall on the issue of interoperability, Admiral Metcaft [the CINC of Atlantic Command and the overall commander of the operations], 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."[7]

These and other articles revealing 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 subject of interoperability. The need of the military to address this situation that could cost lives in combat 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 Combatant Commanders.[8] The interoperability situation was starting to get some visibility, and the policies regarding the conduct of warfare started to look more joint in nature. Five years later, our military would face interoperability challenges again in the aftermath of Suddam Hussein's invasion of Kuwait.

PERSIAN GULF WAR

Operations 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. The Persian Gulf war also tested our progress regarding equipment design to ensure interoperability. As in Grenada, the mission 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.[9]

Former Secretary of Defense Les Aspin and Representative William Dickerson, 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 incompatibility and technical limitations. At U.S. Central Command (CENTCOM) 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….[10]

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 differences in planning tools used by the Air Force and the joint community and those used by the Army in setting up the TRI-TAC communications nodes. The Army used the acquisition program's objective network planning 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 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.[11]

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 (JFACC) in charge of prosecuting the air war and air tasking used the air tasking order (ATO) as a centralized planning and execution product, 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

transported to the fleet by helicopter or tactical jet. Interoperability is challenging and proved to be a continuing concern for future operations conducted in Africa.

SOMALIA

Operation Restore Hope (Somalia, 1991) also revealed interoperability barriers among U.S. forces. The lessons learned from this operation 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 a joint environment."[14] The Marines Air Ground Task Force 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 Navy and Marine Amphibious Ready Group. The most serious instance reported was an incompatibility in single –channel tactical radios. The use of different equipment upgrades resulted in problems severe enough to prevent the Army hospital in Mogadishu from being able to talk to the Navy offshore for the three weeks of the operations.[15]

There are many more examples of operations including Operations Desert Fox, the operations in Kosovo and even the ongoing operations in Afghanistan. Although our military has made significant progress, the lessons learned reports from Afghanistan are very likely to reveal more of the same interoperability challenges that history has shown us.

WHAT IS INTEROPERABILITY?

Interoperability is a very broad and complex subject. It is far more difficult than the binary attribute of single system operation. C4I interoperability is a key enabler for the conduct of effective, collaborative, and multi-service military operations across a wide spectrum of scenarios, and successful conduct of operations is the ultimate test of whether an adequate degree of interoperability is being achieved. The DoD Directive 5000.1 defines interoperability as "The ability of systems, units, or forces to provide services to or access services from other systems, units, or forces, and use the services to operate effectively together".[16]

Joint Chiefs of Staff Publication 1-02 defines interoperability at both the technical and operational level. Operational interoperability addresses support to military operations and, as such, goes beyond systems to include people and procedures. It is the ability of systems, units, and forces to provide services to and accept services from other systems, units, and forces, and to use the services so exchanged to enable them to operate effectively together. It addresses interacting on an end-to-end basis. Implementation of operational interoperability implies not

only the traditional approach of using standards, but also enabling and assuring activities such as testing and certification, configuration and version management, and training. These definitions of operational interoperability encompass the full spectrum of military operations, including intra-service/agency, joint (inter-service/agency), and ad hoc and formal multinational alliances.[17]

Interoperability at the technical level is essential to achieving operational interoperability. It is the condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.[18] Technical interoperability focuses on an issue that arises between systems rather than between organizations. Technical interoperability must be considered in a variety of contexts and scopes, even for a single mission. Consider the theater missile defense mission, which is likely to require that data be:

- *Exchanged among elements of a weapon system.* For example, the Patriot air defense system uses a defined message format and data link to exchange information within batteries and between batteries to share target information and coordinate defensive actions.
- *Exchanged between weapons systems of a single organization or service.* For example, the Theater High Altitude Area Defense system (under development) will provide theater ballistic missile tracks to Patriot systems.
- *Exchanged between weapons systems of different services.* For example, a Navy AEGIS radar may report tracks to an Army Patriot radar.
- *Shared and "pooled" at the joint task force command and control systems level (or higher) in order to achieve synergy and added value.* For example, Patriot, AEGIS, and Airborne Warning and Control System data may be combined to develop a common operating picture and to control and coordinate all the systems sharing data.

The range of complexity of requirements for data flow in such a mission underscores the significance of interoperability at every level. [19]

One source of interoperability problems is incompatibilities in independently selected versions (e.g., software releases) of the same system. Thus, if one unit has standardized on version A of a given system and another on version B, capabilities supported by one system and not the other may well interfere with seamless interoperation between the two units. In 1995 at Fort Hood Texas, this very example was illustrated when the III Corps commander

questioned why the Army's Maneuver Control System (MCS) was having trouble sharing information between the units of III Corps. It was discovered that III Corps, I Cavalry Division, 4th Infantry Division and the Army's Communication Electronic Command (CECOM) all had different versions of the MCS software. Software interoperability is not an uncommon cause of system non-interoperability in Army systems, and can be complicated even more when working in the joint environment. Also, just as differences in modes of operation across the services can lead to non-interoperability, so can organizational differences within a service also lead to intra-service incompatibilities.

When thinking about C4I it is important to understand the distinction between joint systems and systems that are interoperable. A system can be designated as joint either to support an efficient buying decision for two or more services that will use it, or because the system will be subject to joint command. By contrast, to meet requirements for interoperability, services' systems must be able to share data in a timely, reliable manner that is operationally useful, and must operate across service or agency boundaries to support joint missions.

The goal of joint C4I interoperability is operational and technical interoperability commensurate with the role of C4I in support of multi-unit, joint, and combined missions. Joint, flexible, and coherent operations are key components of DOD's vision (e.g., Joint Vision 2020) meaning operational interoperability of forces and technical interoperability of C4I systems. Future U.S. military operations will inevitably involve elements from more than one service. Forces will probably be assembled with minimal time for planning and deployment, in ad hoc configurations, and for geographically far-flung missions that are highly diverse compared to those undertaken during the Cold War. Operation Enduring Freedom in Afghanistan is a perfect example of the complex and unpredictable nature of warfare we are sure to face in the future. To enable fast and effective responses, interoperability must be built into the force structure across service and unit boundaries.

WHY IS INTEROPERABILITY SO IMPORTANT?

To fully realize the concept of Joint Vision 2020 one must first understand that the future vision is predicated on a concept of information superiority. That Information superiority is enabled and supported by a network of C4I systems--one whose constituent elements interoperate and cooperate to support the entire warfighting hierarchy, in the context of joint and coalition operations. 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.

Interoperability is important because experience in operations such as Desert Storm and Bosnia, as well as evidence from recent experiments and exercises, points to the dramatic improvements in operational effectiveness that are achievable using highly capable C4I systems. Our future warfighting doctrine is centered on information dominance enabled by highly capable C4I systems. The leverage provided by a common operating picture and the rapid decision-making ability associated with it can dramatically change the pace, nature, and geographic range of engagement, providing major advantages to forces so enabled. Interoperability is important because it is absolutely the key to realizing these advantages.

Interoperability is also an important factor in operational efficiency. Where interoperability is lacking, there is always the likelihood that multiple systems are performing the same functions, or that information is being manually entered or processed multiple times. Additionally, lack of interoperability also means that personnel have to resort to work-around methods. Where interoperability is not in place, the necessary transfer of information between systems may require speaking over a voice link or rekeying data from printouts or handwritten notes. These processes are not only inefficient but they are often error-prone as well.[20]

Military operations are typically joint, requiring that the C4I systems of multiple services work together effectively. Both the generally unpredictable nature of military contingencies and the wide range of non-traditional operations mean that forces and weapons are likely to be combined in novel, unanticipated ways to meet operational requirements and that their C4I systems may need to interoperate in ways not explicitly planned for in advance. Also, the new operational emphasis on rapid force projection, and the concept of early entry to halt an invasion, means that there will likely be less time during a deployment to fix interoperability problems. Finally, the increasing size of the area over which combat operations take place--and thus the number of possible forces and weapons that must coordinate their attack--means that data is increasingly being exchanged between sensors, weapons, and systems that previously operated in a stand-alone manner. To meet such operational requirements, the different elements of the C4I system of systems will need to be more interoperable.[21]

Many important military missions require a high degree of interoperability to support cross-service collaboration. Some specific instances in the area of joint operations include the following:

- Close air support, which requires that ground troops be able to communicate their air support needs to ground attack airplanes in a timely and accurate fashion;

- Suppression of enemy air defenses, which in general requires the coordinated use of missiles and aircraft operated by multiple services;
- Theater missile defense data may be shared between weapons systems of different services or shared at the joint task force command and control systems level (or higher);
- Regional air defense, which requires the coordination of many air defense assets, from missile batteries and radar on the ground to airborne surveillance platforms and air defense fighters; and
- Deep-strike attacks and interdiction of enemy forces behind the front lines, which both require the coordinated use of airspace, strike aircraft, ground, and sea-based missiles, and long-range artillery.

In short, interoperability is essential to operability--that simply means that forces cannot operate effectively without a high degree of interoperability among their systems. That said, universal interoperability is neither achievable nor necessary. Not every C4I system on the battlefield needs to interoperate with every other one. Nor is universal interoperability--which might be thought of as allowing all information in all systems to be seamlessly exchanged and interpreted--technically feasible, given the rate of change in both technologies and missions.[22]

Unfortunately interoperability, when considering system acquisition is often treated as a potentially desirable but nonessential element of C4I programs. Sufficient degrees of interoperability, especially inter-service, are often not currently seen by managers as a pass-fail criterion for their programs. Consequently, interoperability requirements can often be one of the first things sacrificed when budgets force program cost reductions.

WHY ACHIEVING INTEROPERABILITY IS DIFFICULT

It would be easy to fix the challenges of interoperability if one person, one office, or one institution could be held responsible. The interoperability situation did not occur overnight, and the people, offices, and institutions involved with the processes have all changes several times, leaving no single person or organization to blame. Factors and combination of factors contribute to the persistent shortcomings that are routinely reported in interoperability. Experience in the private and military sectors suggests that the following factors (among others) often operate to inhibit or slow the achievement of desired system interoperability.

SYSTEM ACQUISITION CULTURE

One of the first factors that affect 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 Combatant Commander staffs –the originating Combatant Commander and Commander, United States Joint Forces Command as the advocate for interoperability; the service staff responsible for acquiring the system; and numerous other defense agencies, including the Joint Interoperability Test Command (JITC), which is responsible for testing and certifying the system as interoperable. Adding in Congress, defense contractors, and lobbyists and the inefficiency becomes apparent—and inevitable.[23] This culture unfortunately is very difficult to control and has led to an environment with significant and unfortunate effects on achieving interoperability.

TENSION BETWEEN IMMEDIATE AND FUTURE NEEDS

Operational units (in the DOD context, the Combatant Commanders as the warfighting authorities) in an organization often have a perspective very different from that of the planning units (in the DOD context, e.g., the Office of the Secretary of Defense, Joint Chiefs of Staff, and the service chiefs as the policy makers, allocators of resources, and providers). Operational units are concerned with the capabilities of today's systems in the short term, whereas planning units are concerned with the capabilities of tomorrow's systems, over the longer term.

For the planner, interoperability is a capability that must be designed into a system. For the operator, interoperability is often achieved by working around problems, e.g., deciding what parts of a system to use or not use, creating patches, and modifying policy or doctrine associated with its use. For the planner, changes in system capability (i.e., changes in feature and function) are important. To the operator, changes in operating capability (perhaps enabled by changes in deployed system capability) have greater significance. For the planner, operational doctrine and tactics are driven by what can be imagined when the force is fully equipped and the new technology or system is deployed. For the operator, operational doctrine is driven by deployment of a system and the resulting capabilities of the unit.

Units and organizations recognize that operational considerations (e.g., training, doctrine) must be an integral part of system acquisition. Maintaining such a focus is difficult when operators believe that planners are not rapidly responsive to their immediate needs. Planners believe that an overemphasis on immediate needs will not enable operating units to fully realize the benefits of new capabilities.

Optimizing overall system performance requires a full understanding of the trade-offs entailed by different choices. Individual units within an organization, especially those that

seldom interact with other service units, are strongly motivated to solve their own pressing C4I problems. These units proceed in solving the problems, as they deem necessary, even if doing so makes it harder for them to interact with other service units. In addition, the fact that many acquisition programs have very long time lines increases the pressure to deploy independently developed solutions. The result of such independent development is very often a patchwork of systems that are even less interoperable.

LAGACY SYSTEMS

Legacy systems are and will remain a fact of life for the military. As units modernize and generations of C4I technology succeed one another, the new systems will have to interface with legacy systems. The major challenge presented by legacy systems is the cost of upgrading all of the systems. It is financially and organizationally impossible to upgrade or replace the vast inventory of command, control, communication and computer systems and the associated training required for the systems. The rapid changes in technology have hampered interoperability because it is difficult to achieve interoperability and continue to leverage the benefits of technology. It is also unrealistic for the military armed services to ignore the vast potential advantages technology can provide. The legacy interoperability challenge with new C4I technology is even more challenging when considering the capability of potential adversaries to access the same technology. The technological advantage enjoyed by the United States is slowly being diminished as technology is proliferated around the world. The global world and advances in technology demand that our acquisition process strike a workable balance between new and legacy C4I technology.

CURRENT POLICIES

There are many policies that govern and address C4I interoperability for the organizations and agencies within the Department of Defense. The general nature of these polices are to provide guidance regarding the total system approach to the acquisition of systems and programs. The policies address C4I standardization, how operational requirements are generated, certifications, test and evaluations among many parameters.

DEPARTMENT OF DEFENSE POLICIES.

Directive of Defense Directive (DoDD) 5000.1, “Defense Acquisition,” and Department of Defense (DoD) Instruction 5000.2, “Operation of the Defense Acquisition System,” dated October 23, 2000 provide guidelines, roles, and responsibilities for implementers within the Department of Defense. DoDD 5000.1 provides policies and principles for all DoD acquisition

programs. It establishes a disciplined management approach for defense acquisition to assist the Under Secretary of Defense for Acquisition, Technology, and Logistics (USDAT&L); the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)); and the Director, Operational Test and Evaluation (OTE) in meeting their fundamental commitments as the department's decision authorities for acquisition programs. DoDD 5001 also provides specific policy guidance on translating operational needs into stable affordable programs, and identifies responsibilities for key officials within the DoD. DoDD 5000.1 applies to the Defense Department, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, DoD Field Activities, and all organizational entities within the DoD.

The combination of the directive and regulation provide those responsible for implementation with broad and sweeping authority affecting the entire life cycle of DoD system acquisition. Further, for the first time, acquisitions for information and weapon systems are found within the same directive and regulation. However, it provides no guidance that would assist in the determination of where policy ends and implementation begins. To further examine the C4I process for system interoperability a look at the joint policies is required.

JOINT POLICIES

The DoD has embraced the joint culture as a dominant imperative for conducting warfare in the future. Military organizations can no longer afford to develop and acquire systems that are not aimed at joint interoperability. History has shown that joint interoperability and the requirement to meet joint and regulatory guidelines are essential to the success of the military in the future.

Joint requirements are defined as requirements that impact more than one DoD component. All C4I and intelligence, surveillance, and reconnaissance (ISR) systems for purposes of compatibility and interoperability and integration are considered joint. Programs having a joint potential designator (JPD) of joint or programs designated as "joint" will become more numerous over time and need to be developed with participation of all DoD components.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 dated 15 April 2001 is the primary joint instruction establishing policy guidance for joint and regulatory guidelines for system acquisition. The purpose of CJCSI 3170.1 is to establish policies and procedures for the requirements generation of new systems. It provides policies and procedures for developing, reviewing, validating, and approving Mission Need Statements (MNSs) and Operational Requirements Documents (ORDs). It provides policies and procedures for developing,

reviewing, validating, and approving Capstone Requirements Documents (CRDs). CJCSI 3170.1 delegates oversight authority for the requirements generation system to the Vice Chairman of the Joint Chiefs of Staff, assisted by the Joint Requirements Oversight Council (JROC) and members of the Joint Staff.

It additionally provides guidelines for the conduct of requirements and program reviews at each milestone for Major Defense Acquisition Programs (MDAPs) prior to their being forwarded for Defense Acquisition Board (DAB) review and Major Automated Information System (M01AIS) acquisition programs prior to their being forwarded to Assistant Secretary of Defense (Command, Control, Communications and Intelligence) ASD (C3I) or appropriate component acquisition executive and JROC. CJCSI defines the role of the JROC Secretary as the Joint Staff point of contact for the submission, handling, and review of MNSs, and CRDs, and the CJCSI provides policy guidance regarding the following roles and responsibilities:

- Authority. The Chairman of the Joint Chiefs of Staff assesses military requirements for defense acquisition programs and represents the Combatant Commanders with respect to their operational requirements. The JROC facilitates the execution of these responsibilities.
- Service Role. The Services are responsible for organizing, supplying, equipping (including research and development), training, administering, and related functions in order to meet the current and future operational requirements of the unified commands. They are also charged with eliminating duplication through effective cooperation and coordination with the other Services and DOD agencies.
- CJCS Role. The Chairman of the Joint Chiefs of Staff, assisted by the Vice Chairman and other members of the Joint Chiefs of Staff, establishes and publishes policies and procedures governing the requirements generation system.
- VCJCS Role. The Vice Chairman of the Joint Chiefs of Staff, assisted by the JROC, will oversee the requirements generation system in accordance with DOD 5000 series documents and policies and procedures contained in this instruction to ensure the responsibilities of the Chairman under title 10, USC, are fulfilled.
- DoD Chief Information Officer (CIO) Role. The DoD CIO is responsible to ensure the interoperability of information technology and national security systems throughout the Department of Defense. DoD CIO will ensure that information technology and national security systems standards that will apply throughout the Department are prescribed and

provide for elimination of duplicate information technology within and between the Military Departments and Defense agencies.

ARMY POLICIES

The U.S. Army in a policy memorandum signed by LTG Peter Cuviello, Army Chief Information Officer (CIO, G6), and dated 3 December 2000, revised its Intra-Army Interoperability policy. The policy memorandum outlines and establishes an intra-Army interoperability certification requirement for communications/data interfaces for all Army operational-through tactical-level command, control, communications, computers and intelligence (C4I) systems.

Under the provisions of the DOD Directive (DODD) 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems, November 12, 1992 and the Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6212.01B, Interoperability and Supportability of National Security Systems and Information Technology Systems, May 8, 2000, the Joint Interoperability Test Command (JITC), a component of the Defense Information Systems Agency, conducts joint level interoperability certification and recertification testing for C3I systems. This testing currently applies to C3I systems only (reference Army Regulation 73-1, Test and Evaluation Policy, February 27, 1995, paragraph 4-2b(8) and 4-4b(5)) and is not sufficient for certifying horizontal and vertical interoperability for intra-Army C4I systems at the operational and tactical levels.

Intra-Army interoperability certification applies to all Army operational-through tactical-level C4I systems prior to release to the field, regardless of the acquisition category. Communications/data interfaces testing in support of intra-Army interoperability certification will be addressed in Operational Test Readiness Reviews and considered entrance criteria prior to decision reviews, operational testing, and materiel release. Any modifications that impact previously established interface requirements to fielded systems require re-certification prior to approval for materiel release.

Once a system is certified as interoperable, it is considered a base case system. The Program Manager or System Manager shall make no unilateral changes to the base case system that have the potential of affecting interoperability unless agreed to by the Director, Deputy Chief of Staff for Operations and Plans (DCSOPS) Directorate of Integration. If requested changes are approved, the Program Manager or System Manager must bear the re-

certification cost of all affected systems within a period not exceeding 12 months from date of approval. The following responsibilities are assigned:

- The Director of Information Systems for Command, Control, Communications and Computers will:
    - Serve as the intra-Army interoperability certification authority. The certification authority may be delegated to the system milestone decision authority. All certification actions will be returned to the test facility for distribution and record keeping.
    - Approve the Central Test Support Facility (CTSF) test requirements and criteria for the intra-Army interoperability testing.
- Director, DCSOPS Directorate of Integration is the approval authority for interoperability changes to a base case system.
- The Program Managers and System Managers will program and budget funding for interoperability testing. The Program Managers and Systems Managers, in coordination with the U.S. Army Training and Doctrine Command System Managers, will provide the CTSF with a set of approved test requirements and criteria for intra-Army interoperability testing. Intra-Army interoperability testing and certification will be addressed in the individual program Test and Evaluation Master Plan or in a test concept document.
- The CTSF, operated and funded by Program Executive Office, Command, Control and Communications Systems and located at Ft. Hood, Texas, is identified as the intra-Army interoperability testing facility to perform the communications/data interfaces testing. CTSF testing in support of the intra-Army certification process will not duplicate or limit testing conducted by the JITC, the U.S Army Test and Evaluation Command, or other test activities. The CTSF conducts the required intra-Army interoperability certification testing and provides the test results to the certification authority.

JOINT INTEROPERABILITY TEST COMMAND (JITC)

In the certification process the Joint Interoperability Test Command plays a vital role in ensuring interoperability compliance. The role of JITC is to support the Warfighter in efforts to manage information on and off the battlefield. This includes being an independent operational test and evaluation/assessor of DISA, and other DoD C4I acquisitions. JITC is also responsible for identifying and solving C4I and Combat Support Systems interoperability deficiencies. It provides C4I joint and combined interoperability testing, evaluation and certification bringing C4I interoperability support, operational field assessments, and technical assistance to the Combatant Commanders, Services, and Agencies. It also provides training on C4I systems, as appropriate.

The vision of JITC is to be the preeminent information systems evaluator, reducing risk to the warfighter by providing value-added process and product evaluations, operational assessments, and technical assistance throughout the life cycle of DoD Systems. The JITC testing policy to ensure interoperability is outlined as follows:

> The JITC is responsible for certifying that all Department of Defense C4I systems are interoperable. DoD Directive (DoDD) 4630.5 and DoD Instruction (DoDI) 4630.8 mandate joint and combined interoperability certification testing for "all Command, Control, Communications, and Intelligence (C3I) systems developed for use by US forces." This certification must be obtained prior to fielding a new system. DoDI 4630.8 directs DISA to "develop and conduct a C3I systems interoperability testing and certification program." Further amplification is contained in the Chairman, Joint Chiefs of Staff Instruction 6212.01B. The Director, DISA, delegates this responsibility to JITC. Our principal goal is to establish increased interoperability through a quality, cost effective testing program administered throughout the life cycle of a system. This life cycle starts with the requirements identified during the acquisition phase and continues through the retirement of the system. Certification is based on JITC review and analysis of system requirements, test plans, and test results. Testing may be conducted by JITC or another certified test agency. JITC approval of other agency test plans is required to ensure they meet certification criteria requirements prior to the start of testing.[24]

The JITC is the place for "one-stop systems testing" with a one-of-a-kind array of hardware, software and staffing, along with its state-of-the-art technological flexibility. JITC can interface all its on-site capabilities and network with any other testing or operational facility worldwide.

THE PROCESS TO ENSURE COMPLIANCY

The process that is used to ensure compliancy and interoperability is the use of CJCSI 6212.01. It provides guidance regarding requirements documents generation, system development, system evaluation, fielding decisions, and deployment of systems to provide the Warfighter with joint interoperability. The Joint Interoperability Test Command (JITC) is critical during each phase of the process. JITC can assist in the development of systems, which will require interoperability to work together effectively, and efficiently in the joint battle space. JITC can also tailor the evaluation programs of non-traditional acquisitions to meet certification-testing requirements. JITC follows the processes outlined in CJCSI 6212.01 to perform its joint information interoperability test and certification mission. This mission includes the following efforts:

MISSION NEED STATEMENT (MNS)/CAPSTONE REQUIREMENTS DOCUMENT (CRD).

MNSs are normally received early in a program and are very general in nature with high-level interoperability requirements. CRDs provide the overarching view for Family-of-Systems (FoS)/Systems-of-Systems (SoS). The JITC reviews MNSs/CRDs to determine interoperability requirements with external systems, ensure that identified standards are consistent with the Joint Technical Architecture (JTA), and, if required, that the proposed system can interoperate with Joint, Combined, Coalition, and US components. MNSs and CRDs are provided to the JITC from DISA via the Joint C4I Program Assessment Tool (JCPAT). The purpose of the JCPAT database is to track all requirements documents received by DISA as prescribed in CJCSI 3170.01 and 6212.01. DISA receives documents from the Joint Staff and submits them to other activities via the JCPAT, and maintains an archive of the documents and associated review comments. The JCPAT is an invaluable tool for tracking the status of system requirements documentation, as well as being a valuable information source for the JITC's web-based System Tracking Program (STP).[25]

OPERATIONAL REQUIREMENTS DOCUMENT (ORD).

The ORD is prepared and updated by the system proponent at key phases of the acquisition process. Of primary consideration to JITC are the interoperability requirements defined by CJCSI 3170.01, Requirements Generation System. For interoperability, CJCSI 3170.01 calls for Interoperability Key Performance Parameters (I-KPPs) and Information Exchange Requirements (IERs), besides defining the basic format for MNSs, CRDs, and ORDs. JITC must ensure that these requirements, especially external interfaces to joint systems, are adequately addressed. I-KPPs must be derived from the top-level IERs (basically, the

interoperability interfaces); IERs must include all of the mandatory fields (e.g., event, sending/receiving nodes, type [voice, data, video], and timeliness) and any appropriate optional information (e.g., expected frequency of requests for periodic information such as radar track updates). System design must also conform to the appropriate Joint Architectures, such as the Joint Operational Architecture (JOA) and Joint Technical Architecture (JTA) and standards profiles. Review of these items is critical to the success of both the system and testing, as information at the operational level is eventually expanded and mapped into technical views that form the basis of interoperability T&E and certification. An essential review criterion is that requirements are testable and measurable. Increased accuracy and detail in specifying the interoperability requirements in the ORD are necessary as the system acquisition progresses. Detail to be expected includes standards profiles and specific messaging standards, such as U.S. Message Text Format (USMTF) and Tactical Digital Information Link (TADIL). While interoperability requirements are certified by the Joint Staff, JITC input to the definition process is important to ensure that the T&E mission and interoperability test certification is successful.[26]

C4I SUPPORT PLAN (C4ISP)

The C4ISP provides a mechanism to identify and resolve implementation issues related to an acquisition program's command, control, communications, computers, and intelligence, surveillance, reconnaissance (C4ISR) infrastructure support and system interface requirements. It identifies C4ISR needs, dependencies, and interfaces for programs in all acquisition categories, focusing attention on interoperability, supportability, and sufficiency concerns. The C4ISP describes system dependencies and interfaces in sufficient detail to enable test planning for interoperability key performance parameters (KPPs) and information exchange requirements (IERs). Certification of supportability defined in C4ISPs is likewise a Joint Staff responsibility; however, C4ISPs will play an increasingly important role in JITC business as more programs adopt the new documentation requirements. C4ISPs contain the most detailed view of IERs, and identify what is required from interfacing systems and the supporting communications infrastructures - all of which are items that play a critical part in evaluating interoperability.[27]

TEST AND EVALUATION MASTER PLAN (TEMP)

JITC support activity increases during TEMP development. The TEMP addresses the required interfaces for the system and also indicates the scope and manner in which these requirements are to be examined during the testing process. The JITC TEMP review includes adequacy of technical content and planning for standards conformance testing and interoperability testing, including resources and scheduling. This review ensures the efficient

use of resources and identifies potential scheduling conflicts. JITC participates in the Test Integration Working Group (TIWG), Test Planning Working Group (TPWG), or other working group forums in developing or revising the interoperability testing aspects of the TEMP. The program manager should plan and allocate funds to permit JITC participation in certification testing, as required.[28]

SYSTEM TRACKING PROGRAM (STP)

Per CJCSI 6212.01, JITC maintains a database to track the interoperability and conformance status of programs and systems. Besides satisfying the Joint Staff requirements for tracking certification status, the STP serves to record programs/systems that have created requirements documents, as well as managing JITC's testing schedule. The web-based STP is populated with entire life-cycle information to cover support from initial concept phases to the point where a system is no longer in the inventory. The tracking process starts when initial requirements documents are generated, includes any Interim Authority to Operate (IATO), monitors test scheduling, resources, execution, and reporting events, and culminates with the certification status and recertification notifications. Program Managers and organizations with a requirement for NSS/IT system interoperability certification or other test support should contact the JITC Plans & Policy Branch or their JITC Action Officer for assistance with entering their testing requirements in the STP. STP entries should be made as early in the acquisition process as possible, and updated as testing and evaluation progresses.

DEVELOPMENTAL TEST (DT).

A JITC Action Officer will work with the program management office to determine if the system conforms to the JTA or other applicable standards. Standards conformance testing of a system is performed under the direction of the Program Manager, usually during DT, by one of their contractors or the JITC. Because the JITC does not necessarily conduct all of the testing, JITC must examine other scheduled tests to identify interoperability and conformance data that are available from these sources and what changes in testing may be necessary to satisfy JITC needs. Based on the results of such testing, the JITC will certify that applicable standards and standards profiles have been met. This certification can be expressed in a standards conformance certification letter or listed on a JITC conformance register. If appropriate, component and system interoperability assessments can be used to increase the level of confidence that the system will interoperate when fielded.

OPERATIONAL TEST (OT).

The JITC Action Officer works with the Operational Test Agency (OTA) to ensure adequate interoperability testing is accomplished and suitable data is provided to the JITC for evaluation. Interoperability testing is normally performed in conjunction with OT whenever possible to conserve resources. However, interoperability evaluation will be conducted throughout the life cycle of systems.

JITC can also assist the OTA to obtain the participation of other Services and Agencies required for joint certification. The JITC will report on the information interoperability, and provide the expected operational impact of any interoperability problems. For DISA (and other designated) programs, JITC may also be the OTA. A related function provided by JITC - required by the DoD 5000 series policy - is input into the OT Readiness Review (OTRR). Based on developmental testing and standards conformance results, adequacy of interoperability requirements definition and test planning, and other relevant factors, JITC provides a recommendation as to whether a system is ready for OT.

DoDD 4630.5 and CJCSI 6212.01 mandate Interoperability Test Certification for all National Security Systems (NSS) and Information Technology (IT) systems. JITC's role as DoD's sole agent for Interoperability System Test Certification is to ensure that effective information interoperability exists among interfacing NSS and IT systems. JITC interoperability certification ensures that a system meets user requirements for joint and combined interoperability. Interoperability allows people, procedures, and equipment to operate together effectively and efficiently. The JITC is the center agency for all joint C4I systems to achieve the initial certification that will lead to system interoperability of the battle space for the transforming forces of the future.

USJFCOM'S ROLE

The director for requirements and integration (J8) participates in the allocation of resources at the Department of Defense level to ensure unique joint requirements, such as a combat identification system or a theater missile defense system, are examined for any interoperability issues with existing or planned technologies. Part of this process includes the planning, programming, and budgeting of new systems and prioritizing their assessment by Department of Defense committees such as the Joint Requirements Board, and the Joint Requirements Oversight Council. The J8 serves as the lead joint integration expert, ensuring the various services and defense agencies can combine their capabilities into a single successful effort. This effort allows the services to fight both "joint" (integrated capabilities

between the Marines, Air Force, Army, Navy, etc.) as well as “combined” (U.S. forces and allied militaries fighting as a cohesive package).

Within Joint Forces Command, the director also serves as the deputy for the entire transformation effort, to ensure the integration of the various disciplines (training, experimentation, etc.). Part of this process includes the planning, programming, and budgeting of new systems and prioritizing their assessment by Department of Defense committees such as the joint requirements board, and the joint requirements oversight council.

The integration and interoperability effort is facilitated through subordinate agencies such as the Joint C4ISR (Command, Control, Communications, Computer, and Intelligence, Surveillance, and Reconnaissance) Battle Center – also known as the “JBC”. The JBC serves as a “battle laboratory” for analyzing Department of Defense integration and interoperability issues, and works closely with the joint force trainer’s.

THE FUTURE OF SYSTEM INTEROPERABILITY

Certification of joint interoperability is a complex process requiring the full cooperation of all players in the acquisition community. The achievement of interoperability across a large-scale, complex C4I system of systems supporting military operations is a difficult undertaking. The DoD has undertaken a number of efforts, at multiple levels within the services, the Joint Staff, the Office of the Secretary of Defense, and Defense-wide agencies, to deal with these challenges.

Despite increased attention and management awareness, along with joint and service processes, much more must be done before the infrastructure of C4I systems is as a whole largely interoperable and all new systems are sufficiently interoperable with the appropriate partners. The goal is to provide the interoperability information needed to use systems in the intended operational environment. The transformation efforts of many DoD agencies rest on the ability of the developed system to work in an interoperable environment. Success on the battlefields of the future is greatly dependant on the precious capability that system interoperability can provide.

SUMMARY

Achieving interoperability in a changing world that must also embrace the vision of information operations is a difficult undertaking. The history regarding interoperability is well documented and the resolve of the DoD community is focused on closing the interoperability gap. The DoD C4I systems refinement process is on going. Although much has been done to achieve C4I interoperability, the goal of a C4I system of systems with assured interoperability

for the U.S. military continues to be unachieved. The research in this paper shows that the DoD has devoted significant attention to addressing the interoperability dilemma. The research shows that the procedures and processes are in place.

Interoperability challenges continues to hit hard at all levels of operations. When our military is called to duty, the operational and tactical levels are impacted greatly. Perhaps one of the most significant of all the processes for the operational and tactical users is the JITC process. If it were the priority of all of the tactical and operational level users to simply ensure that all newly acquired C4I equipment achieve JITC certification, many of the interoperability challenges and much of the interoperability discovery learning on the battlefield would not exist. The DoD processes and procedures require disciplined commanders and staffs at all levels asking tough interoperability questions regarding the acquisition process and of the contractors that supply our government system. Our commanders and staffs should force candid answers to one simple question; “Are newly acquired systems and equipment JITC certified for interoperability?”

Although the DoD has made and continues to make great progress in the general nature of interoperability, every operational conflict reminds and teaches us why interoperability is so important. The DoD faces major challenges to assure effective exploitation of C4I systems. Progress in some cases has been slow, and past C4I studies show that many documented C4I interoperability problems remain unresolved.[29]

It is understood that the lead for developing C4I architectures is a shared responsibility of many. If we are to achieve the imperatives outlined in Joint Vision 2020, tackling the interoperability challenge must be among the top priorities for the DoD. One of the best ways to prepare for an uncertain future is for DoD to develop the capacity to rapidly understand situations as they unfold. Warfighters will need an ability to quickly bring resources to bear in a responsive way that will transcend the full spectrum of military operations. Interoperability will definitely be one of the golden keys to future operational success. Successful transformation of the Army and other DoD agencies as we face the challenges of the twenty first century will absolutely depend on unlocking the elusive key to interoperability.

WORD COUNT = 8,870

ENDNOTES

[1] William S. Cohen, "Secretary of Defense Report to Congress: Actions to Accelerate the Movement to the New Workforce Vision," 1.April 1988; available from <http://www.defenselink.mil/pubs/foi/err.html>; Internet; accessed 15 January 2003.

[2] Jacques S. Gansler, Arthur L. Money, Philip E. Coyle, and Scott A. Fry, Memorandum for Secretaries of the Military Department, 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, "Interoperability: Is it achievable," 19 January 2001; available from <http://www.research.maxwell.af.mil/papers/students/ay2001/affp/faughn-pdfl>; Internet; accessed 15 February 2003.

[4] Chairman of the Joint Chiefs of Staff [CJCS], Joint Vision 2020 (Washington, D.C.: U.S. Government Printing Office, June 2001.

[5] Hillman Dickinson, "Planning for Defense-Wide Command and Control," December1982; available from <http://www.research.maxwell.af.mil/papers/students/ay2001/affp/faughn-pdfl>; Internet; accessed 15 February 2003.

[6] Frank M. Snyer, Command and Control: The literature and Commentaries (Washington, D.C.: National Defense University Press, 1993), 111.

[7] Stephen Anno and William E. Einsahr, "The Grenada Invasion," available from <http://www.fas.org/man/dod-101/ops/urgent fury.html>; Internet; accessed 25 January 2003.

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

[9] 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).

[10] Frank M. Snyer, Command and Control: The Literature and Commentaries (Washington, D.C.: National Defense University Press, 1993), 79.

[11] Center for Army Lessons Learned," Interoperability," January 1992; available from <http://www.call.army.mil/products/newltrs/92-1/92-1ch3.html>; Internet; accessed 15 January 2003.

[12] Department of the Navy, "Lessons Learned and Summary," *U.S. Navy in Desert Shield/Desert Storm, Quick Look: First Impressions Report*, 22 March 1991, available from <http://www.history.navy.mil/wars/dstorm/ds6.htm>>; Internet; accessed 15 February 2003.

[13] Ibid.

[14] C. Kennth Allard, “Operational Lessons Learned: Somalia Operation”, available from <http://www.dtic.mil/doctrine/jel/jfg_pubs/2409.pdf>; Internet; accessed 15 February 2003.

[15] Ibid.

[16] Department of Defense Directive 5000.1, "Defense Acquisition," 15 March 1996; available from <http://www.acq.osd.mil/ar/doc/dodd5000-1.pdf>; Internet; accessed 15 February 2003.

[17] U.S. Joint Chiefs of Staff, “Department of Defense Dictionary of Military and Associated Terms,” 7 December 1998; available from <http://www.acq.osd.mil/ar/doc/dodd5000-1.pdf>; Internet; accessed 15 January 2003.

[18] Ibid.

[19] “Realizing the Potential of C4I, Fundamental Challenges, “available from <http://wwwnap.edu/html/C4I/notice.html>; Internet; accessed 9 January 2003.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Anthony W. Faughn, “Interoperability: Is it Achievable?” Program on Information Resources Policy; 23 October 2002, available from <http://www.research.maxwell.af.mil/papers/students/ay2001/affp/faughn-pdfl>; Internet; accessed 9 February 2003.

[24] Defense Information System Agency, “JITC Testing Policy,” available from <http://jitc.fhu.disa.mil/policy.htm>; Internet; accessed 9 February 2003.

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] General Accounting Office, “Joint Military Operations: DOD’s Renewed Emphasis on Interoperability Is Important But Not Adequate,” available from <http://www.globalsecurity.org/intel/library/reports/gao/150094.pdf>; Internet; accessed 9 February 2003.

BIBLIOGRAPHY

Alberts, David S. Information Age Transformation. Washington, D.C.: DoD Command and Control Research Program, June 2002.

Alberts,David S, John J.Garstka, and Frederick P. Stein. Network Centric Warfare. Washington, D.C.: DoD C4ISR Cooperative Research Program, February 2000.

Alberts, David S. etal. Understanding Information Age Warfare. Washington, D.C.: DoD Command and Control Research Program, August 2001.

Allard, Kenneth C. "Operational Lessons Learned in Somalia Operations: Lessons Learned." Washington, D.C.: National Defense University Press, 1995. Available from <http://www.ndu.edu/ inss/bookds/allardch2.html>. Internet. Accessed 25 February 2003.

Anno Stephen and William E. Einsahr. "The Grenada Invasion." 1988. Available from <http://www.fas.org/man/dod-101/ops/urgent fury.htm>. Internet. Accessed on 25 January 2003.

Center for Army Lessons Learned. " Interoperability." January 1992. Available from <http://www.call.army.mil/products/newltrs/92-1/92-1ch3.html>. Internet. Access on 15 January 2003.

Clinton, William J. A National Security Strategy for a Global Age. Washington, D.C.: The White House, December 2000.

Cohen, William S. Secretary of Defense Report to Congress: "Actions to Accelerate the Movement to the New Workforce Vision." Department of Defense, Washington, D.C.: 1988.

Cuviello, Peter M., Army Acquisition Executive Director of Information Systems for Command, Control, Communications, and Computers Director of Information. "Intra-Army Interoperability Certification." Memorandum: Washington, D.C. 3 December 2000.

Defense Information System Agency. "JTIC Testing Policy." Available from <http://site.fhu.disc.mil/policy.html>. Internet. Accessed 9 February 2003.

Dickinson, Hillman. "Planning for Defense-Wide Command and Control." December 1982. Available from <http://research.maxwell.af.mil/papers/students/ay2001/affp/faughn.pdf>. Internet. Accessed 15 February 2003.

Douglas, Gordon and Tran, Phuong. "Joint Interoperability Certification." Joint Interoperability Test Command (September-October 1999): 24-27.

Faughn, Anthony W. "Interoperability: Is It Achievable?" Program of Information Policy Research. Harvard University. October 2002.

Gansler, Jacques S. Memorandum for Secretaries of the Military Department, 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. Washington, D.C., 4 Dec. 2000.

Money, Arthur. “Message from the Assistant Secretary of Defense Command, Control, Communications, and Intelligence.” Available from <http://www.C3i.osd/mil/infosaper/message.html>. Internet. Accessed 24 February 2003.

Myers, Richard B. Remarks to the AFCEA TechNet International 2001 Luncheon. Washington, D.C.: U.S. Joint Chiefs of Staff. 6 June 2001.

Phillips, David W. Interoperability Available from <http://www.ndu.edu/inss/macnair/machair18/m018ch01.html>. Internet. Accessed 15 February 2003.

Phillips, David W., Joint C4ISR [Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance] Decision Support Center. Interviewed by author Jan, 2001. Crystal City, Virginia.

“Realizing the Potential of C4I, Fundamental Challenges,” Available from <http://www.nap.Edu/CSI/notice.html>. Internet. Accessed 9 March 2003.

Shelton, Henry H. Enabling the Joint Vision. Posture Statement, Washington, D.C.: U.S. Joint Chiefs of Staff. June 2000.

Shelton, Henry H. Joint Vision 2020. Washington: U.S. Joint Chiefs of Staff, June 2000.U.S. Army War College. Information Operations Primer. Carlisle Barracks: U.S. Army War College, Department of Military Strategy, Planning and Operations. January 2002.

Snyer, Frank M. Command and Control: The Literature and Commentaries, Washington, D.C.: National Defense University Press, 1993.

U.S. Department of Defense. “Drivers of Change.” Available from <http://www.C3i.osd.mil/Infosuper/NewEnviron.html>. Internet. Accessed 29 February 2003.

U.S. Department of Defense. “Information inn War.” Available from <http://www.C3i.osd.mil/Inforsuper/InfoWar.html>. Internet. Accessed 23 February 2003.

U.S. Department of Defense. Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs, Department of Defense Regulation 5000.2R. Washington, D.C.: U.S. Department of Defense, 10 June 2001.

U.S. Department of Defense. The Defense Acquisition System. Department of Defense Directive 5000.1. Washington, D.C.: U.S. Department of Defense, 23 October 2000.

U.S. Department of Defense. “The Way Ahead.” Available from <http://www.C3i.osd.mil.infoSuper/wayAhead.html>. Internet. Accessed 23 February 2003.

U.S. Department of Defense. “Why is Information Superiority Important?” Available from<http://www.C3i.osd.mil. infosuper/whyInfo1.html>. Internet. Accessed 23 February 2003.

U.S. Department of the Navy. “Lessons Learned and Summary.” *U.S. Navy in Desert Shield/Desert Storm, Quick Look: First Impressions Report.* 22 March 1991. Available from <http://www.history.navy.mil/wars/dstorm/ds6.htm>. Internet. Accessed on 15 January 2003.

U.S. General Accounting Office. “Joint Military Operations: DOD’s Renewed Emphasis on Interoperability Is Important But Not Adequate.” Available from <http://www.globalsecurity.org/intel/library/reports/gao/150094.pdf>. Internet. Accessed 9 February 2003.

U.S. Joint Chiefs of Staff. “Department of Defense Dictionary of Military and Associated Terms.” 7 December 1998. Available from <http://www.acq.osd.mil/ar/doc/dodd5000-1.pdf>. Internet. Accessed 15 January 2003.

U.S. Joint Chiefs of Staff. “Director for Command, Control, Communications, and Computer System – Mission and Functions.” Available from <http://www.dtic.mil/jcs/J6/m-and-f.html>. Internet. Accessed 28 January 2003.

U.S. Joint Chiefs of Staff. “Joint Vision 2020.” Washington, D.C.: U.S. Government Printing Office, June 2001.

U.S. Joint Chiefs of Staff. Requirements Generation System. CJCSI 3170.01B. Washington, D.C.: U.S. Joint Chiefs of staff Joint Chief of Staff, 15 April 2001.

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.