NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

EXAMINATION OF AUTOMATED INTEROPERABILITY TOOLS FOR DoD C4I SYSTEMS

by

David L. Ruiz
Richard E. Williams

September 2000

Thesis Advisor:	Rex Buddenberg
Associate Advisor:	John Osmundson

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2000	**3. REPORT TYPE AND DATES COVERED** Master's Thesis Sepetember 2000	
4. TITLE AND SUBTITLE: Title (Mix case letters) Examination of Automated Interoperability Tools for DoD C4I Systems			**5. FUNDING NUMBERS**
6. AUTHOR(S) Dave Ruiz, Maj USMC; Richard Williams, Maj USMC			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

This thesis examines the ability of C4I systems within DoD to exchange information in the operational battlespace. With the advent of the Information Age and resultant development of the strategy of network-centric warfare, interoperability has become increasingly significant as a criterion for mission success, while also becoming increasingly difficult to achieve as well. The PPBS cycle bears some responsibility for this by creating competition amongst the Services for finite resources, perpetuating the environment that contributes to "stovepipe" C4I systems development. This thesis examines DoD's attempts to solve the interoperability dilemma by using policies and procedures. We demonstrate that a cooperative effort among components, services, and agencies to integrate methodologies within PPBS should enhance the efforts of planners and developers in designing interoperability through the integration of C4ISR architecture development processes. As a part of this examination we will also evaluate several automated software tools that have been designed to facilitate interoperability, and present recommendations as to how these tools could be integrated to complement their effectiveness within the requirements generation and capabilities development processes.

14. SUBJECT TERMS Interoperability, JCAPS, MSTAR, LISI			**15. NUMBER OF PAGES** 182
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXAMINATION OF AUTOMATED INTEROPERABILITY TOOLS FOR DoD C4I SYSTEMS

David L. Ruiz
Major, United States Marine Corps
B.S., United States Naval Academy, 1985

Richard E. Williams
Major, United States Marine Corps
B.A., Illinois State University, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2000

Authors:

David L. Ruiz

Richard E. Williams

Approved by:

Rex Buddenberg, Thesis Advisor

John Osmundson, Associate Advisor

Dan C. Boger, Chairman
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines the ability of C4I systems within DoD to exchange information in the operational battlespace. With the advent of the Information Age and resultant development of the strategy of network-centric warfare, interoperability has become increasingly significant as a criterion for mission success, while also becoming increasingly difficult to achieve as well. The PPBS cycle bears some responsibility for this by creating competition amongst the Services for finite resources, perpetuating the environment that contributes to "stovepipe" C4I systems development. This thesis examines DoD's attempts to solve the interoperability dilemma by using policies and procedures. We demonstrate that a cooperative effort among components, services, and agencies to integrate methodologies within PPBS should enhance the efforts of planners and developers in designing interoperability through the integration of C4ISR architecture development processes. As a part of this examination we will also evaluate several automated software tools that have been designed to facilitate interoperability, and present recommendations as to how these tools could be integrated to complement their effectiveness within the requirements generation and capabilities development processes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

ACE	Air Combat Element
ACOM	Atlantic Command
ACTD	Advanced Concept Technology Demonstration
ASD	Assistant Secretary of Defense
ASN	Assistant Secretary of the Navy
BE	Budget Execution
C/S/A	Component/Service/Agency
C4I	Command, Control, Communications, Computers, & Intelligence
C4IFTW	C4I for the Warrior
C4ISR	C4I Surveillance and Reconnaissance
CADM	Core Architecture Data Model
CAPS	Command Acquisition Programs System
CECOM	Communications-Electronics Command
CII	Compatibility, Interoperability, and Integration
CinC	Commander in Chief
CIO	Chief Information Officer
CIPO	CinC Interoperability Program Office
CJCS	Chairman Joint Chiefs of Staff
CJCSI	CJCS Instruction
CMM	Capabilities Maturity Model
COE	Common Operational Environment
COI	Critical Operational Issues
ConOps	Concept of Operations
COTS	Commercial-off-the-Shelf
CRD	Capstone Requirements Documents
CSSE	Combat Service Support Element
CTP	Common Tactical Picture
DASD	Deputy Assistant Secretary of Defense
DBMS	Database Management System
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DPG	Defense Planning Guidance
E-to-E	End to End
FMF	Fleet Marine Force
GAO	General Accounting Office
GCCS	Global Command and Control System
GCE	Ground Combat Element
GIG	Global Information Grid
HTML	Hypertext Markup Language
I-KPP	Interoperability Key Performance Parameter

ICEP	Interoperability Certification Evaluation Plan
IE	Information Elements
IER	Information Exchange Requirements
IOC	Initial Operational Capability
IP	Internet Protocol
IPL	Integrated Products List
IPTP	Interoperability Policy Test Panel
JC2I2G	Joint Command and Control Integration and Interoperability Group
JCAPS	Joint C4I Architecture Planning/Analysis System
JFCOM	Joint Forces Command
JFPO	Joint Forces Program Office
JIEO	Joint Information and Engineering Organization
JIT	Joint Interoperability Tool
JITC	Joint Interoperability Test Command
JMTIRA	Joint Maritime Tool for Interoperability Risk Assessment
JOA	Joint Operational Architecture
JROC	Joint Requirements Oversight Committee
JSPS	Joint Strategic Planning System
JTA	Joint Technical Architecture
JTAMDO	Joint Theater Air and Missile Defense Organization
JTF	Joint Task Force
JV2020	Joint Vision 2020
LAN	Local Area Network
LISI	Level of Information Systems Interoperability
MAGTF	Marine Air Ground Task Force
MARCORSYSCOM	Marine Corps Systems Command
MCCB	Management Configuration Control Board
MCCDC	Marine Corps Combat Development Command
MCEB	Military Communications Electronics Board
MCTSSA	Marine Corps Tactical Systems Support Activity
MDA	Milestone Decision Authority
MEB	Marine Expeditionary Brigade
MEU(SOC)	Marine Expeditionary Unit (Special Operations Capable)
MIP	MAGTF Integrated Package
MNS	Mission Need Statements
MSTAR	MAGTF C4I Systems Technical Architecture and Repository
NMS	National Military Strategy
NSS	National Security Strategy
ONCD	Operational Node Connectivity Description
OPFAC	Operational Facility
ORD	Operational Requirements Documents
OSD	Office of the Secretary of Defense
PAID	Procedures Applications Infrastructure and Data
PM	Program Manager

POM	Program Objective Memorandum
PPBS	Planning Programming and Budgetary System
R-to-C	Requirements to Capabilities
SCD	Systems Communications Description
SHADE	Shared Data Environment
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SoS	Systems of Systems
TAFIM	Technical Architecture Framework for Information Management
TCP/IP	Transfer Control Protocol/Internet Protocol
TEMP	Test Evaluation Master Plan
TRM	Technical Reference Model
USD	Under Secretary of Defense
WAN	Wide Area Network
WWW	World Wide Web
XML	Extensible Markup Language
Y2K	Year 2000

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to show our appreciation to all the faculty that instructed us over the 28 months we attended the Naval Postgraduate School, particularly Rex Buddenberg and LtCol Terry Brady who together first stimulated our interest in this subject. We would also like acknowledge all the support received from interested organizations, to include Capt Dave Rosen and LCOL Drew Hamilton of JFPO and Maj Ed DeVillers of MARCORSYSCOM. Finally, we would like to thank our families and friends for encouraging us when they needed to and putting up with us when they had to.

Executive Summary

The problem of interoperability is not a new one in the area of warfare. During Desert Storm, US Navy carriers were unable to receive Joint Force Air Component Commander Air Tasking Orders electronically due to bandwidth constraints on satellite connections. Prior to the Gulf War, the USS Vincennes brought down an Iranian commercial airliner after personnel misinterpreted information presented on fire control system displays. As far back as one cares to look, interoperability has played a role in the effectiveness of military command and control operations.

The methodology for examining the degree of interoperability a system exhibits has historically been to test on a "one-to-one" basis with every other system it theoretically could interact with. However, as the number of automated information systems has risen and interoperability requirements begin to converge, the connections between systems that would have to be considered increases exponentially at the rate of $(N^2-N)/2$. Due to this effect, current organizational processes have found it impossible to develop adequate integrating tools and metrics to completely facilitate the design, testing, and certification of C4I systems.

DoD 5000.2-R makes use of the terms compatibility, interoperability and integration, collectively known as "CII". In relation to the other terms, "interoperability" is defined as the ability of systems to exchange services and operate effectively together. "Integration" is generally considered to go beyond interoperability to involve some degree of functional dependence (tighter coupling), while "compatibility" is something

less than interoperability, with systems not necessarily interfering with each other's functioning, but also not implying the ability to exchange services. The continuum created between compatibility, interoperability, and integration provides the requirements generation process a type of referential "baseline" upon which to frame comparisons.

Thankfully, interoperability has been receiving increased attention from the operational community. As forward-looking doctrinal discussions such as Joint Vision 2020 take place, it is becoming apparent that achieving dominance of the "infosphere" requires much more than just having the most advanced information systems.

Interoperability success in the past has come as a result of the one-to-one certification effort and the emphasis on standardization compliance. We have realized for some time that the devil of assuring interoperability is in the details of implementation. The problem we continue to have is that testing and evaluation efforts have been predominately focused on system-centric issues. Certification of system-to-system interfaces does not conclude the integration process; it merely begins it.

The focus of the thesis is to recommend a more integrated way of aligning the organizational and technical aspects available today that define interoperability and to suggest directions for the development of future efforts. We started by examining interoperability policy within DoD. Several publications deal with interoperability, most notably CJCSI 6212.01B and DoDI 4630.8. The problem with these documents is that responsibility for assessing and certifying interoperability was divided amongst different agencies. To compound this problem, none of these agencies was given the authority to intercede in Service acquisition programs if interoperability criteria were not met.

As a part of this process we examined the requirements-to-capabilities (R-to-C) model. The purpose of this was to see where interoperability "fit" in the acquisition cycle. DoD 5000.2-R and CJCSI 3170.01A both address this R-to-C cycle. The dilemma in this area is that requirements are having a difficult time keeping up with technology, vice the other way around that we have observed in the past. Operational forces (the warfighters) have difficulty effectively expressing their needs within the context of emerging technology to the development and acquisition communities.

How DoD addresses these problems was our next phase of analysis. The Joint Technical Architecture, Global Information Grid, and Defense Information Infrastructure Common Operating Environment all point towards the need for an all-encompassing "system-of-systems" (SoS) concept, defined as mission-based integrated C4I systems that are scalable, driven by common standards, and can share information transparently within their own SoS as well as between different SoSs.

DoD is still nowhere near a global information structure that is interoperable. We found several reasons for this failure, but, as might be expected, the Planning, Programming and Budgeting System (PPBS) was the main culprit. This system encourages competition amongst the services for limited resources. To maintain control of their own funding Services develop their own programs, often contrary to another Services programs. Such "stove-piped" acquisition programs breed interoperability problems from their conception to their fielding and beyond.

Another problem we examined is the interoperability certification process. The Joint Interoperability Test Command is the DoD agency responsible for certifying

systems interoperability. The problem with their approach is that the thrust of the certification effort is still focused on the operational testing of one-to-one interfaces with little regard to SoS affiliation or mission-defined functionality. We did discover that strides are being taken to address this, specifically through the efforts of integration efforts of the U.S. Joint Forces Command.

Finally, though Services are becoming increasingly concerned with interoperability, they do not currently have the tools to assess, test, and construct interoperable architectures. Several agencies within DoD are taking steps to correct this deficiency. We looked at several of these agencies and what processes/tools they were developing. The Joint Staff J-6 is the sponsor for the Joint C4ISR Architecture Planning/Analysis System (JCAPS), the most mature and capable of the currently available tools, as well as the automated Levels of Information Systems Interoperability (LISI) Inspector tool. The Marine Corps Systems Command is developing a central database for C4I architectures known as the MAGTF C4I Systems Technical Architecture and Repository (MSTAR) that would assist in developing integrated C4I "go-to-war" architectures. SPAWAR Systems Charleston is developing the Joint Maritime Tool for Interoperability Risk Assessment (JMTIRA), a tool that assesses risk associated with interoperability problems.

What is required is an overarching model of where these tools fit in the larger C4I development process, and then to determine how they can be employed synergistically. All of the tools showed promise but will require further development and integration. We determined that the best elements of each tool should be integrated into one system that

could address interoperability in the entire requirements generation process. Embedding such a tool within the R-to-C model would provide a collaborative and comprehensive development environment that would greatly benefit C4I system interoperability in spite of the inherent limitations of the DoD acquisition and PPBS cycles.

I. INTRODUCTION

> Without major strides in the area of interoperability we will not achieve the information superiority essential to realizing Joint Vision 2010.
>
> RADM Robert Nutwell
> DASD(C3ISR&S)
> 10 April 2000

A. PURPOSE

The purpose of this thesis is to examine the interoperability of Command, Control, Communications, Computers, and Intelligence (C4I) systems within the Department of Defense (DoD). Interoperability is a problem as old as combat itself; with the advent of the Information Age and resultant development of the strategy of network-centric warfare, interoperability has become increasingly significant as a criterion for mission success, while at the same time becoming more and more difficult to satisfactorily achieve. Various organizations and procedures dealing with interoperability have been caught in an evolutionary cycle, first attempting to define the interoperability "battlespace" and then to formulate an overarching framework that brings some semblance of order to it. This thesis examines several of these initiatives, comments on their effectiveness and future potential, and suggests new ideas that could be implemented to improve C4I system interoperability.

B. BACKGROUND

1. History

The problem of interoperability is not a new one in the area of warfare. During Desert Storm, US Navy carriers were unable to receive Joint Force Air Component Commander Air Tasking Orders electronically due to bandwidth constraints on satellite connections. Prior to the Gulf War, the USS Vincennes brought down an Iranian commercial airliner after personnel misinterpreted information presented on fire control system displays. In Vietnam, Air Force close-air support pilots flying with UHF radios could not talk directly with most Army units, equipped only with VHF sets. At the beginning of World War II, Army Signals personnel detected the Japanese attack force 130 miles from Pearl Harbor utilizing radar, but an Air Corps watch officer, skeptical of the capabilities of the newly developed technology, discounted the report and took no actio: As far back as one cares to look, interoperability has played a role in the effectiveness of military command and control operations. However, the more important implication is that as we begin to look forward, we are finding that not only is interoperability becoming an increasingly vital commodity, but that the "boundaries" of the problem seem to be expanding at a rate greater than our ability to solve it.

2. Joint Vision 2020

The Chairman, Joint Chiefs of Staff (CJCS) doctrinal publication Joint Vision 2020 (JV2020) states:

> The basis for this new conceptual framework for operations is found in the improvements that can be assured by information superiority. Enhanced Command & Control

> and much improved intelligence, along with other applications of new technology, will transform traditional military functions. These transformations will be so powerful that they become, in effect, new operational concepts: dominant maneuver; precision engagement; full-dimensional protection; and focused logistics. In combination, these will provide our forces with a new conceptual framework: full-spectrum battlespace dominance.

The actualization of this vision is heavily predicated on the assumption that information superiority has already been effectively achieved. As we become increasingly dependent on networked forces to implement this strategy, we are finding that it is just as much about the interoperability of technology as the individual technologies themselves that becomes the principal enabler of combat power.

As advanced systems in the acquisition pipeline are fielded and legacy systems receive upgrades to extend and enhance their service life, interoperability issues are becoming increasingly complex. The methodology for examining the degree of interoperability a system exhibits has historically been to test on a "one-to-one" basis with every other system it theoretically could interact with. However, as the number of automated information systems has risen and interoperability requirements begin to converge, the connections between systems that would have to be considered increases exponentially at the rate of $(N^2-N)/2$. Due to this effect, current organizational processes have found it impossible to develop adequate integrating tools and metrics to completely facilitate the design, testing, and certification of C4I systems.

3. The GAO Reports

a) GAO/NSIAD-87-124

In 1987 the General Accounting Office (GAO) completed *"DoD's Efforts to Achieve Interoperability Among C3 Systems"* at the request of the House Committee on Government Operations.[1] This report cited three primary causes for interoperability problems:

- Decentralized management structure.
- Lack of clearly defined joint requirements.
- Absence of effective enforcement authority to make interoperability decisions.

The fundamental recommendation of the report introduced the concept of **certification** of a system's interoperability as a prerequisite to its being developed and procured, and specifically outlined the withholding of appropriated funds from programs that did not comply with this new certification process.

b) GAO/NSIAD-94-47

Seven years later, this time at the request of the Secretary of Defense, GAO published *"DoD's Renewed Actions To Improve C4I Interoperability May Not Be*

---

[1] United States General Accounting Office. "Interoperability: DoD's Efforts to Achieve Interoperability Among C3 Systems". GAO/NSIAD-87-124.

Adequate".[2] This report highlighted the importance of **architecture** (i.e. the structure and relationship among the components of a system) in achieving interoperability while reaffirming that much of the earlier report's findings were still problematic. DoD's "C4I for the Warrior" (C4IFTW) initiative, as it was called at the time, had been published two years prior as a result of Gulf War lessons learned. C4IFTW was designed to address many of those same problems. The GAO report concluded that C4IFTW:

- Showed a prolonged phased implementation process extending over ten years.
- Relied on unproven technological advances with unknown costs.
- Was highly dependent on a yet-undeveloped comprehensive joint C4I architecture.

GAO found that many of the intrinsic problems with the process of interoperability could be traced back to the contentious relationship between the military service components (Army, Navy, Air Force, Marines) and the joint command structure. Not only were traditional operational areas of tactics and doctrine being negotiated between these entities but as a result of the information revolution, technological issues would now also have to be considered.

To address this dichotomy between service and joint priorities, the GAO report included several recommendations. First among these was the idea that all developmental C4I systems should be "born joint"; i.e. that all design specifications would now originate from within the joint requirements structure vice that of the

---

[2] United States General Accounting Office. "DoD's Renewed Actions To Improve C4I Interoperability May Not Be Adequate". GAO/NSIAD-94-47.

individual services. It was hoped that this paradigm shift would serve to reduce the interoperability problems that were introduced by service-defined and service-specific information exchange standards.

Another of the GAO recommendations that related to the services/joint issue was to minimize the reliance on "ad hoc" assembly of information systems. GAO's observations concluded that much of the challenge of interoperability came from the inability of DoD to adequately define which sets of systems would be required to function together. While this recommendation was a bit simplistic at the time, given the changing face of the military mission and the increasing importance of flexible task-based structuring of forces, it did bring to light another of the weaknesses of the interoperability effort; with joint task force organization becoming more necessity than choice, the requirement was identified for a baseline architecture that would facilitate this ad hoc process, as well as automated tools to design and test the functionality of these emergent "systems of systems" (SoS). Future U.S. military operations will inevitably be joint, involving elements from more than one service, often assembled with minimal time for planning and deployment in dynamic configurations for highly diverse missions. Achieving this sort of C4I interoperability is inherently a horizontal, cross-functional challenge that must be addressed in a largely vertical, single-source developmental world.

C4IFTW was one of the first integrated attempts to define this type of required interoperability architecture. The Defense Information Systems Agency (DISA) was given the lead in this effort, and its Joint Interoperability and Engineering

Organization held primary responsibility for technical development. Known as the Joint Tactical C3 Architecture, this early attempt at defining the interoperability battlespace came under sharp criticism. Program Managers (PMs) and the warfighting community alike found the product too abstract for planning purposes, out-of-date upon its issuance, and generally lacking in detail and operational perspective.

A complementary requirement to an interoperability architecture is a mechanism for the enforcement of compliance. GAO again identified this as a problem area for DoD. At the time of the report's publication, there was no organizational entity that could act as a joint program management authority to fill this particular void. GAO recommended the creation of such an organization, one that would be empowered in the budgetary process to influence program funding based on interoperability certification requirements.

The final recommendation of GAO in 1994 was the assignment to the US Atlantic Command the role of interoperability "integrator", consisting of the following responsibilities:

- Assess C4I requirements for potential effect on joint task force operations.
- Provide guidance to DISA on development of the joint C4I architecture.
- Ensure continuous C4I interoperability assessment through joint training exercises.

This initiative was rejected by DoD at the time as being of little value added, stating that validation and compliance issues should reside at the Joint Staff level and architecture remain the sole purview of DISA.

c) GAO/NSIAD-98-73

The House National Security Committee requested that GAO follow-up on its 1994 report, and in 1998 it published *"Weaknesses in DoD's Process for Certifying C4I Systems' Interoperability"*.[3] This document was a scathing indictment of the failure of DoD's interoperability efforts over the past ten years. The primary focus of the report was the interoperability certification process as outlined in the various DoD directives and instructions. GAO found that certification remained ineffective for a variety of reasons.

First among these certification problems was that compliance with the applicable set of interoperability documents, as they were written at the time, could not be implemented. As the saying goes, "the law is on the books, but it would take all their resources to enforce it". While stated DoD policy required that all new or modified systems be certified or obtain a waiver from certification testing prior to proceeding past Milestone III (Production or Fielding/Deployment Approval), GAO found that many systems were proceeding to these latter acquisition stages without being certified, approved by the very same oversight authorities who were also charged with enforcing the certification requirements.

The Joint Interoperability Test Command (JITC), established in 1989 by DISA to be the sole certification agent of C4I interoperability, had no real organizational

---

[3] United States General Accounting Office. "Weaknesses in DoD's Process for Certifying C4I Systems' Interoperability". GAO/NSIAD-98-73.

authority to compel PMs (who answered to the individual services) or the acquisition milestone decision authorities (who often were not required to comply with DoD-level guidance) to require that systems be presented for testing nor to enforce its findings and recommendations when systems were submitted. It was the finding of the GAO that PMs often knowingly did not submit systems for testing, believing their programs would in all likelihood proceed more smoothly and quickly if they did not.

Another problem encountered in certification efforts was that within an acquisition system's Planning, Programming, and Budgetary System (PPBS) cycle, interoperability testing line items often became prime targets for reduction or all-out cuts from a variety of "mark-up" authorities. This was caused in great part due to a lack of knowledge and understanding concerning the interoperability process throughout the budgetary cycle and particularly to a lack of a centralized "champion" of the interoperability cause. Exacerbating this situation was the fact that due to the nature of interoperability not only did the system in question need to provide adequate funding for its own certification testing, but many yet-to-be identified systems would also be required to set aside their own budgetary authority in support as well.

4. Present Day

Interoperability continues to be a difficult issue to address within DoD. Many successful efforts have been implemented, but at times it has seemed that as one problem is solved two more arise to replace it. As with any sort of knowledge, the more we discover about interoperability the more we find out how much we still have to learn.

Our understanding, tools, and procedures are the best they have ever been and are improving all the time, yet the size and scope of the problem they are intended to address is increasing as well. Cutting-edge technologies often sit idly by at the pier or flight line because they cannot work together. To draw an analogy, DoD grows the best vegetables in the world, yet we still have a difficult time making a salad.[4]

C. RESEARCH QUESTIONS

Principle Research Question:

- Is a totally interoperable C4I system attainable, or even desirable, in the joint operational environment?

Secondary Research Questions:

- What is the current interoperability assessment and certification process?
- What are the strengths/weaknesses of available automated interoperability tools?
- How do the assessment tools compare?
- How can the assessment tools be integrated?
- How can the interoperability assessment process be innovated to improve performance of C4I systems in the joint operational environment?
- How can the interoperability assessment process be better integrated into the acquisition cycle?

[4] Buchanan III, H. Lee, ASN(RD&A). Speech. 18 Jul 00.

D. METHODOLOGY

The methodology used in this research consists of the following steps:

- Conduct a literature search on interoperability definitions, OSD policies, and service policies.
- Conduct interviews of key players in the relevant agencies, focusing on their efforts and their interpretations of interoperability policy.
- Collect information from the Interoperability Conference hosted by JITC in April 2000.
- Conduct an analysis of how interoperability fits into the current acquisition cycles.
- Conduct an analysis of the available automated interoperability assessment tools.
- Synthesize interoperability tools into acquisition and certification processes.
- Draw conclusions and make recommendations based on the experiment.

E. ORGANIZATION

Chapter I provides insight into the environment of interoperability as well as introduces some of the significant concepts in this area. Chapters II and III examine administrative issues regarding interoperability and the various attempts by DoD to come to grips with the problems surrounding it. Chapters IV and V provide a review, comparison, and proposed integration of various automated stand-alone tools that have been developed to address interoperability. Chapter VI provides a listing of conclusions, recommendations, lessons learned, and areas for further study.

F. BENEFITS OF STUDY

The focus of the thesis is to recommend a more integrated way of aligning the organizational and technical aspects available today that define interoperability and to suggest directions for the development of future efforts. General readers of this paper will gain an understanding of the underlying issues that have plagued interoperability efforts in the past, become acquainted with current efforts to address these issues, gain an understanding of the factors that affect the state of interoperability efforts, and evaluate the potential effectiveness of future interoperability initiatives. The conclusions and recommendations put forth as a result of this research will be made available to organizations presently involved with the interoperability certification process, specifically at the Marine Corps Systems Command and the Joint Command and Control Integration and Interoperability Group's Joint Forces Program Office.

II. INTEROPERABILITY ISSUES

> The pace of technological change, especially as it fuels changes in the strategic environment, will place a premium on our ability to foster innovation in our people and organizations across the entire range of joint operations.
>
> CJCS Joint Vision 2020 Publication
> June 2000

A. INTRODUCTION

Joint Vision 2010 was an attempt to anticipate the future of warfighting by assimilating the improved C4I capabilities available in the information age, stressing technological innovation as the means to enable interoperable DoD systems. Joint Vision 2020 encompasses more than just information technology, expanding into all aspects of joint force application, thereby intensifying the overall importance interoperability plays in mission success.[5]

The purpose of this chapter is two-fold. The first objective is to provide an overview of the various orders and directives that pertain to DoD interoperability. Specifically, the following documents will be discussed:

- DoD Regulation 5000.2-R: Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs; 11 May 99.
- DoD Instruction 4630.8: Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems; 18 Nov 92.

---

[5] CJCS Publication. "Joint Vision 2020". http://www.dtic.mil/jv2020/

- CJCS Instruction 3170.01A: Requirements Generation System; 10 Aug 99.
- CJCS Instruction 6212.01B: Interoperability and Supportability of National Security Systems, and Information Technology Systems; 08 May 00.

The second part of the chapter presents the PPBS process as it pertains to interoperability, introducing several of the standardization and architectural initiatives being utilized within DoD, to include the Defense Information Infrastructure Common Operating Environment (DII COE), Joint Technical Architecture, and the C4ISR Architecture Framework.

B. DEPARTMENT OF DEFENSE INTEROPERABILITY DOCUMENTS

1. DoD Regulation 5000.2-R – 11 May 99

a) Interoperability in the Acquisition Process

DoD 5000.2-R puts forth policies for all DoD acquisition by establishing a simplified and flexible framework for translating mission needs into affordable, well-managed programs. Its purpose is to provide overarching guidance for the entire acquisition process. The current regulation is a recently published version of the original 5000-series instruction issued in 1991. It is undergoing major revision, with interoperability specifically identified as one of the primary areas of review.[6]

One of the significant changes to the regulation focuses on integrating interoperability considerations into the time-phased framework of current acquisition

---

[6] Nutwell, Robert, RADM, DASD(C3ISR&S). "New Interoperability Policies and Processes". Presentation.

strategy. PMs are instructed to place special emphasis on the transition of interoperability requirements between phases as the overall project progresses through the acquisition management lifecycle.

b) Standardization Initiatives

System engineering techniques such as interface control, open systems design, and the use of standards such as the DoD Technical Reference Model (TRM) are identified as tools to assist in maintaining the integrity and validity of interoperability requirements as they proceed through the different acquisition phase transitions. In March 2000 the TRM replaced all versions of the Technical Architecture Framework for Information Management (TAFIM) as DoD's official standardization policy document.[7]

The TRM is not a specific system architecture; rather it defines services, interfaces, and relationships used in support of technical architecture/interoperability framework development. The purpose of the TRM is to provide a common conceptual framework that defines an accepted vocabulary of architecture terminology as well as providing a high-level description of the information technology domain. A primary objective of the TRM is to establish a context for understanding how to relate the disparate technologies needed to implement information management. The TRM reference model defines a **target** technical environment for the acquisition, development, and support of DoD information systems. The TRM is by necessity a "living" document;

---

[7] Gansler, J., USD(AT&L). "Promulgation of DoD TRM Version 1.0". DoD Memorandum dtd 21 Mar 00.

it contains an evolving set of comprehensive protocols and definitions to support emergent systems and applications as well as including consideration for interoperability requirements in regards to migration and legacy initiatives when such capabilities are deemed essential for mission continuity and accomplishment. All DoD components and agencies have been tasked with revising their respective architectural views based on the new TRM.

c) Compatibility, Interoperability, and Integration

DoD 5000.2-R makes use of the terms compatibility, interoperability and integration, collectively known as "CII". In relation to the other terms, "interoperability" is defined as the ability of systems to exchange services and operate effectively together. "Integration" is generally considered to go beyond interoperability to involve some degree of functional dependence (tighter coupling), while "compatibility" is something less than interoperability, with systems not necessarily interfering with each other's functioning, but also not implying the ability to exchange services. The continuum created between compatibility, interoperability, and integration provides the requirements generation process a type of referential "baseline" upon which to frame comparisons.

2. DoD Instruction 4630.8 – 18 Nov 92

a) Compatibility, Interoperability, and Integration Procedures

DoDI 4630.8 is the implementation instrument for policies outlined in DoD Directive 4630.5 "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems". It assigns responsibilities to

organizational roles/functional areas as well as prescribing procedures for the execution of CII compliance. These procedures define how to develop, acquire, and deploy C4I systems to meet the essential CII needs of US forces. An important distinction made in this instruction is that, for purposes of CII, all C4I systems developed for use by US forces are considered to be "joint", the implication being that individual service sponsors can no longer "stovepipe" systems for exclusive use.

b) Chairman of the Joint Chiefs of Staff

One of the specific roles outlined in this instruction is that of the Chairman of the Joint Chiefs of Staff (CJCS). CJCS is given the responsibility of approving and documenting changes to doctrinal concepts and associated operational procedures that will have CII implications, effectively consolidating this authority at the joint level. The procedure for achieving this within the PPBS is observed during requirements validation (Milestone 0 – Approval to Conduct Concept Studies) and certification testing (Milestone III – Production or Fielding/Deployment Approval).

c) DISA

Another of the set of responsibilities presented in DoDI 4630.8 is that of the Defense Information Systems Agency (DISA). Re-designated in 1991 (formerly the Defense Communications Agency), DISA's primary function in the interoperability arena is that of being DoD's single point of contact for the development of information technology standards. It is DISA policy to maintain a list of approved interface standards

with which new and existing command & control, weapons, and automated information systems must be in compliance.

The mission of DISA, via its Joint Information and Engineering Organization (JIEO) sub-command, is to provide and maintain DoD technical architectures and standards. JIEO's Center for Standards is the DoD's executive agent for the centralized management of information technology standards and was originally responsible for producing the TAFIM as an aid in C4I system configuration management. The Center for Standards is also involved in the development, coordination, and adoption of commercial standards. Another JIEO activity, the Center for Integration, provides support services such as product integration and technical compliance testing, to include metrics collection and analysis of hardware/software and network performance, primarily focused on Global Command and Control System (GCCS) applications.

One of DoD's long-term objectives is to develop a global C4I infrastructure that can accommodate the widest possible range of missions and operational scenarios by allowing users to enter the infrastructure at any time or place.[8] In theory, this "network of networks" or Global Information Grid (GIG) will be constructed upon the foundation that DISA's standardization program provides. The GIG, which is proposed as an all-encompassing globally integrated networking operations weapon system, will provide for "assured interoperable communications"

---

[8] Nutwell, Robert, RADM, DASD(C3ISR&S). "New Interoperability Policies and Processes". Presentation.

among several military systems that carry out varying missions ranging from peace to wartime operations. If realized, the GIG will sustain interoperability by providing information exchange standardization for user and source components. DISA's efforts at developing this capability rely heavily on the management of interface definitions, i.e. the point at which one system must exchange information with another system or network of systems.

3. CJCSI 3170.01A – 10 Aug 99

a) Interoperability Requirements Cycle

CJCSI 3170.01A provides policy guidance into all aspects of DoD's requirements generation system. The requirements generation system is the process that provides decision-makers with information on current and emergent operational needs, and then provides the planning and documentation to effectively translate these needs into the PPBS and acquisition management lifecycles.

b) Need/Requirement/Capability Flow

Commanders in Chief (CinCs), in their role as "warfighter", are the primary initiators of the requirements generation process. Based both upon experience and forward-looking analysis, Mission Need Statements (MNSs) are developed to fill emergent gaps in our warfighting capabilities. A MNS is a non-system specific document written in broad operational terms. These MNSs provide the background for the formulation of Capstone Requirements Documents (CRDs). CRDs capture

overarching requirements (to include interoperability) for entire operational mission areas, such as Combat Identification or Theater Air & Missile Defense.

CRDs are developed when a well-defined function requires multiple systems, some of which may have been developed by different service components, a relationship also known as a "system of systems" (SoS). A single system is typically defined as a set of different elements connected or related so as to perform a unique function not achievable by the elements alone, while a SoS extends this construct by replacing *element* with *system.* CRDs are intended to assist in the development of Operational Requirements Documents (ORDs) by providing a standardization environment that must be complied with by all elements identified as members of a particular SoS.

c) Key Performance Parameters

The ORD is a document containing operational performance requirements for an individual concept or system that define the proposed capabilities needed to satisfy a MNS. Systems that are described in ORDs are defined in terms of Key Performance Parameters (KPPs). KPPs are the capabilities or characteristics considered essential for mission accomplishment and are constructed in terms of measurable threshold and objective values. It is interesting to note that since CRDs are defined by function and ORDs are defined by system, there is a "many-to-many" relationship between them.[9] A

[9] Rosen, David, Capt, JFPO. "Defining the Interoperability Battlespace". Presentation.

CRD will generally require a set of ORDs (representing the SoS) to implement the defined functionality and an individual system ORD may have membership in multiple CRDs. ORDs must be able to trace their KPPs back to every CRD supported, and the CRD must have a relationship defined for every ORD in its SoS, introducing a combinatorial problem to requirements management.

CJCSI 3170.01A mandates the inclusion of a stand-alone interoperability Key Performance Parameter (I-KPP) in all CRDs and ORDs. Within each ORD an Information Exchange Requirements (IER) matrix identifies all the elements of information to be shared by any two or more systems. IERs are the primary measure used in defining the I-KPP values in both CRDs and ORDs. In CRDs, IERs are defined as those information exchanges that are between the systems that make up the SoS as well as those that are external to the CRD's domain, while for ORDs, IERs are only those information exchanges that are external to the individual system. CRD IERs should not be construed as imposing any specific material solution, but are designed to identify the basic characteristics of the information that needs to be present in order to support the functionality defined by the CRD. CRD I-KPPs, and hence the IERs that the I-KPPs are derived from, are measurable, while ORD I-KPPs must be measurable and as well as testable in support of the certification process.

d) Requirements into Capabilities

The operational needs identified by the user community in the MNS, having been transformed into requirements in the CRDs and ORDs, are now sent to the

component Program Management or System Program offices for development and production. It is at this point in the requirements generation cycle that the original warfighter needs begin to take the shape of actual capabilities, signaling the beginning of the acquisition process, and ultimately leading to the fielding of a new/modified system. At the end of this process these systems transfer from the acquisition to the operational community, with the lead service identified during development also typically responsible for its eventual fielding, maintenance, and support.

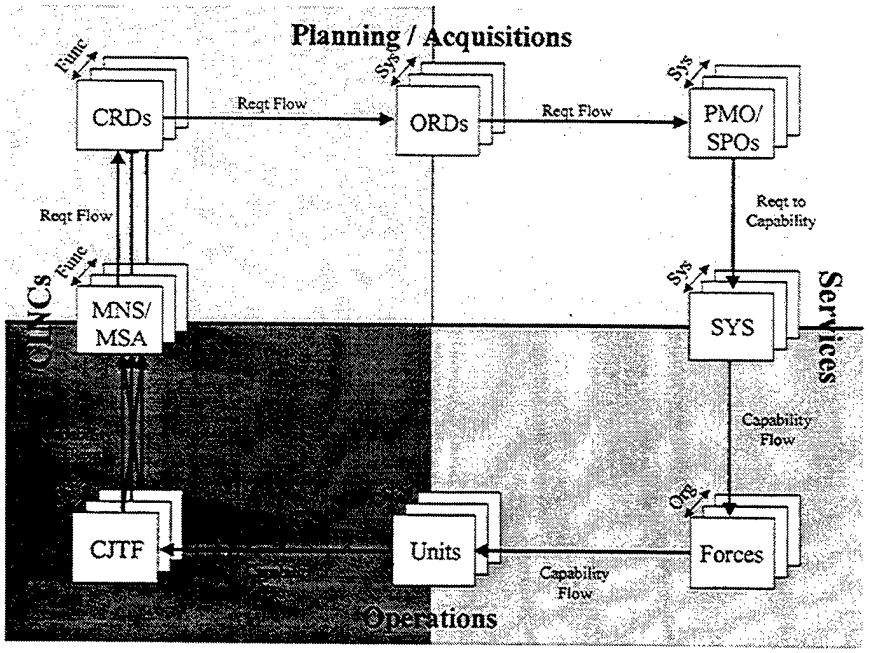

Figure 2-1, Need/Requirement/Capability Cycle[10]

The last link in the overall process occurs when the CinCs, in their roles as Joint Task Force (JTF) commanders, draw upon the component structures for sourcing of

[10] Rosen, David, Capt, JFPO. "Defining the Interoperability Battlespace". Presentation.

the fielded systems in support of a task-organized unit, typically put together utilizing the "ad-hoc" methodology discussed in Chapter I. As these JTFs execute their assigned missions, various shortcomings in capabilities will again become manifest to the CinC staffs, either in response to changes in the perceived external threat or by experience/experimentation with our own tactics and doctrine. This becomes the impetus for the formulation of new MNSs, and the cycle begins again.

4. CJCSI 6212.01B – 08 May 00

a) Overview

This document is the primary reference for all interoperability issues within DoD. It provides inclusive guidance into C4I systems acquisition and the function CII plays in the process. CJCSI 6212.01B outlines the procedures for evaluating MNS and ORD documents, as well as establishes policies to enforce system validation and supportability certification procedures/assessment criteria.

This instruction was first issued in June 1995 and underwent major revision in May 2000 to more closely align it with the provisions of the newly issued CJCSI 3170.01A. One of the more significant modifications was the detailing of the methodology to be utilized in developing KPPs derived from IERs, based on the format of integrated architecture products described in the C4ISR Architecture Framework.

b) Assistant Secretary of Defense as DoD CIO

CJCSI 6212.01B outlines several of the oversight and review responsibilities within the acquisition process. The Assistant Secretary of Defense

(Command, Control, Communications, and Intelligence) is designated to serve as the DoD Chief Information Officer in accordance with the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen). ASD(C3I), serving as DoD CIO, is responsible to the Secretary of Defense for ensuring the cost-effective use of information technology. In this capacity, ASD(C3I) is assigned overarching responsibility for ensuring the interoperability of all information technology and national security systems throughout DoD. This places the CIO function in a position of sufficient authority to ensure that interoperability and standardization programs are complied with throughout DoD as well as focusing on the minimization and elimination of duplicate technologies between the different Components/Services/Agencies (C/S/As).

C. PLANNING, PROGRAMMING AND BUDGETING SYSTEM (PPBS)

Interoperability is problematic within the PPBS for several reasons, all of which point back to the most basic of questions: "Who's going to pay for it?" There are definite costs associated with interoperability, such as the expense of complying with standards and specifications that the individual service components responsible for funding the program do not understand nor see the need for, or for the identification of the many different systems a program will need to be tested against to obtain joint certification.

While interoperability is certainly not free, it stands to reason its cost is much lower if it is considered early during the design phase rather than trying to retrofit it in after the fact, and as has been seen repeatedly, the lack of interoperability has its own associated costs, often much higher than the up-front amounts that historically decision-

makers have been hesitant to justify. What we are willing to pay for interoperability should be linked to the overall value it enables, but this has rarely been the case.

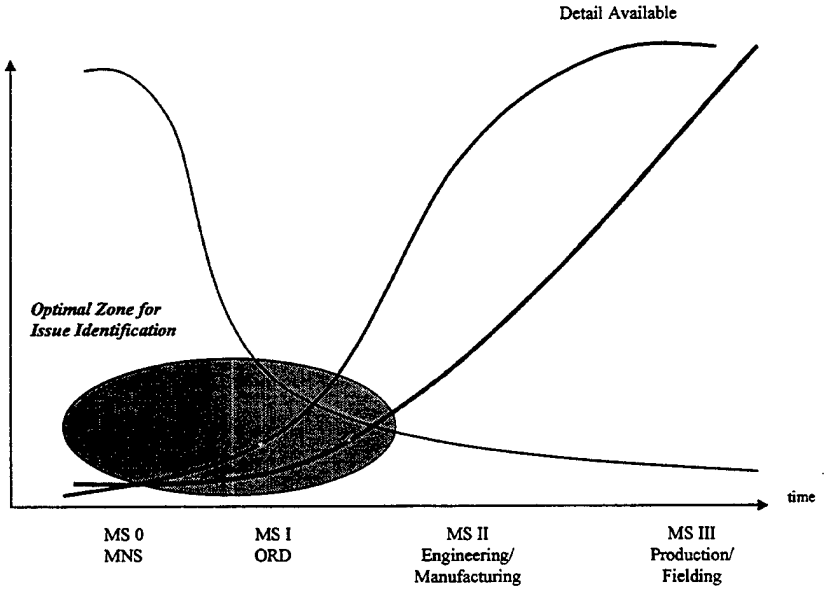

Figure 2-2, "Cost" of Interoperability

While the ability to accurately identify and assess the costs associated with interoperability (or the lack thereof) is problematic, the true crux of the funding conundrum is found within the overall acquisition process itself. The individual DoD service components are the actors responsible for designing, managing, and funding programs. However, often services do not tacitly acknowledge the requirement for "jointness" in its systems, especially if the system does not exhibit interoperability problems within the component's own vertical operational environment.

Another issue that must be considered is the lack of responsiveness within the PPBS itself. Within the framework of the current Program Objective Memorandum

(POM) cycle there exists a three-year lag in obtaining budget approval for new program starts. This delay is benign when dealing with large, industrial end-item procurements such as tanks and planes, but it is fundamentally incompatible with the rapid pace of change seen in information technology. While this is a broader problem than just interoperability, the PPBS process can become a serious impediment to implementing policy even when such policy can be identified and agreed upon. One proposed recommendation to alleviate this situation has been to implement an Interoperability Program Element within the Future Years Defense Program, creating a direct line of funding for interoperability initiatives that is beyond the parochial control of the component acquisition communities.[11]

D. STANDARDIZATION AND ARCHITECTURAL INITIATIVES

1. Defense Information Infrastructure Common Operating Environment

a) DII COE Background

The Defense Information Infrastructure Common Operating Environment (DII COE) is an open architecture designed around the client-server model, analogous to the Microsoft Windows "plug-n-play" paradigm. It provides a set of "off-the-shelf" components and programming standards that describe how to add new functionality to the common environment. The DII COE concept is best described as an architecture that provides an approach for building interoperable systems, a collection of reusable software

---

[11] Nutwell, Robert, RADM, DASD(C3ISR&S). "New Interoperability Policies and Processes". Presentation.

components, and a software infrastructure for supporting mission area applications. The technical architecture developed for GCCS provided the guide for development of the DII COE. All DoD C4I systems and system upgrades are to be DII COE compliant, as outlined in a USD(AT&L) memorandum from August 1996.[12] This memorandum also mandates the use of the Joint Technical Architecture, which references the DII COE as a specific implementation of the JTA that will continue to evolve in compliance with all applicable specifications, standards, and source references.

b) DII COE Components

The DII COE concept is based on a comprehensive definition of the runtime execution environment via a collection of implemented software components. DII COE establishes a methodology for modular software reuse as well as a set of application program interfaces for accessing compliant components. One of the primary DII COE elements is known as the Shared Data Environment (SHADE). SHADE is responsible for data services and other data-related infrastructure that implement sets of shared schema, data management and data access services, build/run-time tools, and technical guidance for supporting COE-based mission applications.[13] The objective of SHADE is to migrate DII COE away from redundant and/or dissimilar data stores to

---

[12] Kaminski, Paul, USD(A&T). "Implementation of the DoD Joint Technical Architecture". DoD Memorandum dtd 22 Aug 96. http://coeeng.ncr.disa.mil/REFERENCE_PAGES/LEV.HTM

[13] Center for Computer Systems Engineering Information Clearinghouse. Shared Data Environment – SHADE. http://dii-sw.ncr.disa.mil/shade/

establish a standardized set of data services built from compliant components that blend multiple data technologies. The Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP) are examples of emerging commercial standards being considered by DII COE to assist in achieving SHADE.

c) DII COE Issues

Drawing on the Windows analogy, the concept of a common operating environment is not as encompassing as it might at first appear. Just as the Windows "plug-n-play" capability certainly has its advantages, it also is not without implementation issues. Interoperability, when viewed from the perspective of interface verification and compliance, should not be considered the conclusion of the integration process but merely the beginning. Even when all individual one-to-one connections have been tested, that does not imply that the SoS is going to function as required by the CRD definition. When integrating C4I architectures, the whole is always different than the sum of the parts. Traditionally, the individual characteristics of a system have been the driving factor in acquisition, leading to the analogy of "stovepipe" development. The key to improving the effectiveness of the SoS as a whole will be to shift the emphasis away from how well a system works and towards how well a system works with other systems, and then finally to how well all the systems work together to accomplish the mission they were grouped together to achieve in the first place.

2. Joint Technical Architecture

The JTA provides DoD systems with the fundamental technical foundation for interoperability. The JTA is structured into service areas based on the TRM that define the interfaces and protocol standards mandated for all developmental projects/existing capabilities that produce, use, or exchange information in any form that electronically crosses a functional or component boundary. Waivers to JTA compliance can only be granted by the Component Acquisition Executive with concurrence from USD(AT&L) via ASD(C3I).

The JTA is essentially a rigidly hierarchical, highly cross-referenced manual document. In its current format, it has proven difficult to implement by designers and programmers due to its inherently "computer-centric" (vice network-centric) focus and ineffective in maintaining relevance to the dynamic commercial marketplace. Alternatives to the JTA, such as object-oriented approaches to DBMS, distributed computing, and programming continue to emerge, but until they are considered "mature and stable" by the DoD Technical Architecture Steering Group they are simply documented in an "Emerging Standards" section of the JTA and are only authorized for use when not in conflict with existing standards. The term "architecture" in JTA is itself somewhat of a misnomer. As a collection of protocols and standards to be complied with the JTA is a relatively useful document; however, it does little to ensure that once individual elements have been assembled into a system that implementation and

functionality decisions will also support interoperability, thus the JTA becomes a part of the puzzle, but not the entire solution.

3. DoD C4ISR Architecture Framework Version 2.1

a) General

The C4ISR Architecture Framework, first published in June 1996 by the DoD Integration Task Force (later revised in July 1998 and again in July 2000), is designed to address a widespread lack of understanding regarding software architecture, often as a result of the use of imprecise terminology. The development of C4ISR architectures is often a distributed process. C/S/As already develop different architectural views for implementations that fall within their specific domains. A common framework and guidance are crucial to achieving C4I interoperability because it is largely a matter of management, design, and implementation discipline between these views rather than simply of resolving technical issues. An interrelated perspective of how these individual architectures combine in the conduct of joint operations does not yet exist in a centralized location, but such a perspective must often be assembled based on emergent joint task force requirements by integrating the various segments produced across DoD.

b) Architectural Views

The C4ISR Architecture Framework defines three descriptive (taxonomic) "views": operational, systems, and technical. The Framework is an attempt to provide guidance in this process of determining and facilitating interoperability amongst these

architectural views.[14] In general, architectures provide a mechanism for understanding and managing complexity. The purpose of C4ISR architectures is to improve the developmental process by enabling the timely synthesis of requirements with fiscal considerations, enabling the efficient production of improved operational capabilities. It is important to note that the Framework is an architectural description vice an architectural implementation. A description is a representation (blueprint) of a postulated configuration, while an implementation is the process of transforming the description into an actual capability.[15]

The operational view is a description of the tasks, elements, and information flows required to accomplish a specific military operation, as defined in the CRD. Operational views define the type of information, frequency of exchange, and tasks supported by the information exchanges. Operational architecture views are generally not system-dependent.

The systems view is a graphical depiction of the interconnections supporting warfighting functions, outlining physical connections such as nodes, circuits, and networks. It specifies overall system as well as individual component performance parameters (interoperability metrics), and shows architecturally how the multiple systems within a CRD-defined mission area domain are linked. The systems architecture view

---

[14] C4ISR Architecture Working Group Final Report.
http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/pdf/fnlrprt.pdf

[15] Manley, James. "Analysis Results of JCAPS Live Fire Test" Conducted by Joint Forces Program Office". MITRE Corporation. December, 1999.

associates physical resource attributes back to the operational view via standards defined in the technical view.

The technical view is the minimal set of rules (services, interfaces, and standards) governing the arrangement, interaction, and interdependence of elements that ensure a conformant system is capable of satisfying a specified set of requirements. Technical views comprise profiles constructed from enterprise specifications, such as those contained in the JTA.

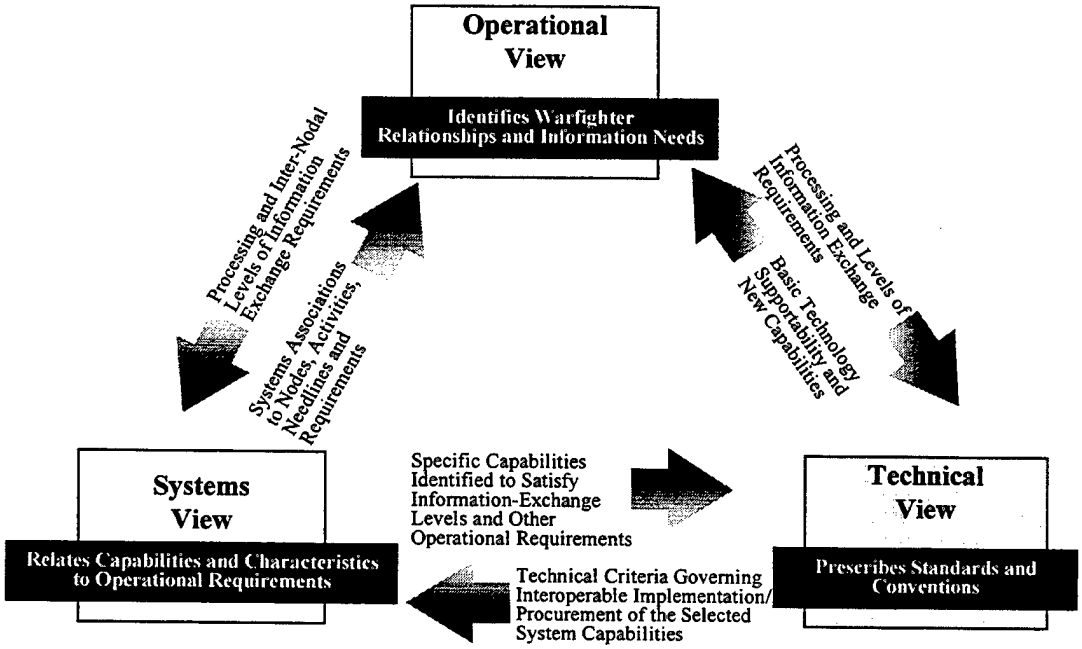

Figure 2-3, Fundamental Architecture Linkages[16]

16 DoD Architecture Framework Working Group. "DoD Architecture Framework Version 2.1, Volume I: Definitions and Guidelines". 26 Jul 00.

To be consistent and integrated, an architecture description must provide explicit linkages among its various views. These linkages provide a cohesive audit trail from operational measures of effectiveness back to the supporting systems' characteristics and specific technical criteria governing their acquisition and development. The operational view describes the nature of these linkages in sufficient detail to determine what specific degree of information exchange is required. The systems view identifies which elements will be used and then compares the required degree of interoperability against the capabilities of the postulated system. The technical view articulates the criteria that should govern implementation of each individual element to achieve the system's overall requirements.

c) Framework Components

The C4ISR Architecture Framework consists of four main components: common definitions, common products, common building blocks, and universal guidance. Common definitions that are used in relation to the three architecture views are clarified and interrelated for understanding and standardization. The common products are notional templates/representation formats that C/S/As will use to describe their C4ISR architectures. Common products that must be developed regardless of specific architecture purpose/scope are identified as "essential", such as the High-Level Operational Concept Graphic, Operational Node Connectivity Description, and Operational Information Exchange Matrix. Several common building blocks, also known as universal reference resources, are included in the Framework. The system architect

does not construct these products but must refer to them to be consistent with prevailing universal guidance and criteria.

An associated product to the Framework is the C4ISR Core Architecture Data Model (CADM). The CADM is complementary as a methodology for providing a common schema for repositories of the architectural views produced by Framework. The CADM provides flexible queries capability in determining the completeness and consistency of the information found in the operational, systems, and technical views.

d) C4I Support Plans

An acquisition tool based upon the C4I Architecture Framework is known as the C4I Support Plan. As soon as possible after Milestone 0 (Approval to Conduct Concept Studies), service components begin identifying C4I infrastructure and support requirements to facilitate the analysis of alternatives during Phase I (Program Definition and Risk Reduction). The purpose of a system's C4I Support Plan is to provide a source of documentation that can be referenced against standardization protocols and compared to baseline requirements, primarily during acquisition lifecycle phase transitions.[17] C4I Support Plans contain progressively more detailed and specific time-phased descriptions of the types of information needed by the developmental system, to include architectural and information exchange requirements, security/connectivity issues, and infrastructure and support shortfalls. This centralized repository allows Program Offices to identify and

---

[17] Dean, Keith, OASD(C3I). "C4I Support Plans (C4ISP) Overview Brief". Presentation. http://www.dsc.osd.mil/dsc/plans/C4ISP_webpg/thebrief.pdf

document system support needs, inter-system dependencies, and interface requirements early in the developmental cycle. Support Plans are required by DoD 5000.2-R for all C4I systems, with waiver authority held at the ASD(C3I) level.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INTEROPERABILITY CERTIFICATION

> If DOD-wide policy alone were sufficient, we would all be programming in Ada today.
>
> LTC Drew Hamilton
> Director, Joint Forces Program Office

A. CERTIFICATION PROCESS

1. Introduction

As a result of the GAO findings discussed in Chapter I, several regulations and instructions have been implemented as well as a variety of organizational entities created/modified. One of the most significant developments brought about was the concept of certification testing. While this certification process has been a considerable step forward in promoting interoperability, it still provides only part of the solution to the overall interoperability question.

In March 2000 the Under-Secretary of Defense (Acquisition, Technology, & Logistics) requested the Director, Operational Test & Evaluation Branch perform an assessment of the current infrastructure supporting interoperability testing to identify capability shortfalls and suggest needed improvements. DOT&E's report found that the need for interoperability is usually acknowledged by the PMs, but detailed requirements, specifically in the form of well-constructed Interoperability Key Performance Parameters (I-KPPs), are generally deemed inadequate.[18] Interoperability testing was found to still

[18]Wallace, Clint, COL. "Preliminary Assessment of Adequacy of Infrastructure Resources to Support Test and Evaluation of Interoperability". Presentation.

concentrate more on examining technical interfaces than on determining the overall mission effectiveness enabled by system interoperability. This ontological gap lies at the heart of the entire interoperability problem. The fundamental question of "What are interoperability requirements in the first place?" continues to go largely unanswered.

2. Certification and Milestone Decision Authorities

"Certification" is a critical step in the development of C4I systems. From the earliest stages of a program's lifecycle, the eventual testing and evaluation of the new system's interoperability must be carefully considered and included in the overall acquisition strategy. The testing process culminates with the issuance of a certification document that will be reviewed by a program's Milestone Decision Authority at Milestone III (Production Approval). Depending on the acquisition category and dollar threshold of the program, the MDA may be:

- USD(AT&L), with advice from the Defense Acquisition Board.
- ASD(C3I), with advice from the Major Automated Information System Review Council.
- Component (such as CinC of a unified combatant command, service chief, or DoD agency head).

The MDA has the responsibility for ensuring that joint interoperability is considered a core competency in overall mission functionality of the system.

According to DoD 5000.2-R, "no new system or system under modification will enter production and gain Initial Operational Capability (IOC) without certification". This certification process also applies to acquisition programs not subject to a formal

review process, such as ACTDs, COTS, and the CinC Initiative Program. The term "system under modification" is rather ambiguously defined as having potential effect at any level of the Open Systems Interconnection protocol.

3. Joint Staff J-6 and the Joint Interoperability Test Command

The J-6 is the organization with primary responsibility for ensuring compliance with interoperability directives, and DISA's Joint Interoperability Test Command (JITC) is the DoD's sole interoperability certification agent. Certification by JITC to the J-6 is confirmation that a C4I system has undergone appropriate level testing to determine if applicable requirements for interoperability have been met and that the system is ready for joint use.[19] JITC certification relies on:

- Review of C/S/A test planning documentation.
- Involvement in all interoperability-related portions of testing.
- Review of analyses prepared by participating test organizations.
- JITC participation in joint exercises, as necessary.

Factors to be considered in the JITC assessment include:

- Ability of the system to operate in a joint environment without degrading operation of other systems or being degraded by them.
- Ability of systems to exchange information and services utilizing applicable standard data elements and formats.

---

[19] JITC Certification Process. http://jitc.fhu.disa.mil/testing/interop/interop.htm

- Ability to interoperate in joint/combined environments without the use of unapproved technical interface devices.

- Ability of systems to maintain required system confidentiality, integrity, and availability.

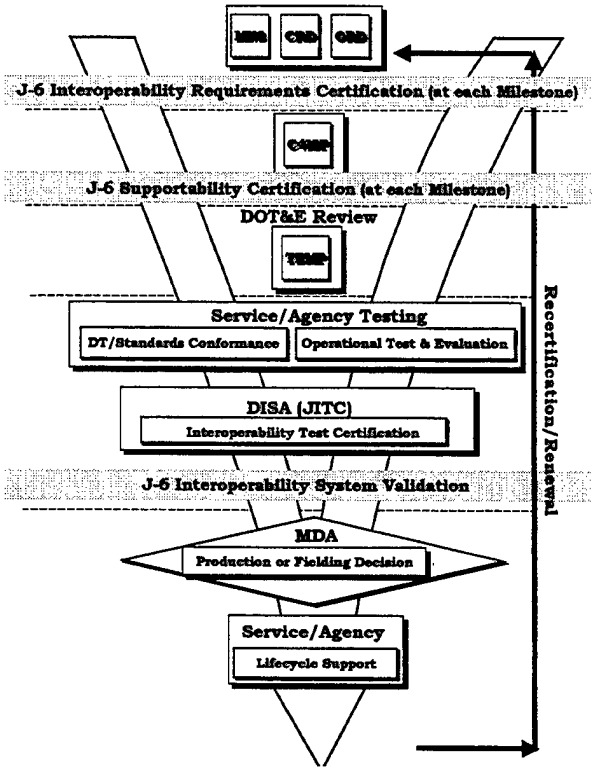

Figure 3-1, Interoperability Test/Certification Process[20]

J-6 ensures that all Mission Need Statements (MNSs), Capstone Requirements Documents (CRDs), and Operational Requirements Documents (ORDs) produced by the requirements generation system are in conformance with National Security Strategy and Information Technology Services policy. J-6 examines all I-KPPs to determine that they

---

[20] CJCS Instruction 6212.01B. "Interoperability and Supportability of National Security Systems, and Information Technology Systems". 08 May 00.

have been accurately derived from the relevant Information Exchange Requirements (IERs), thus providing a participatory function in the certification process while at the same time reaffirming JITC's authority as certification agent. The thrust of J-6's expanded role is to review and validate all CII system test certifications against successful accomplishment of approved mission-based requirements, as defined in the appropriate CRD.

B. CERTIFICATION TESTING

1. Test Planning

The Service Components are generally responsible for funding interoperability certification testing for systems that have not reached IOC). Testing can be conducted by service component test organizations or by JITC facilities during DT&E, OT&E, and/or joint exercise environments. PMs are given the discretion to designate any qualified test organization that best fits budgetary and developmental timeline constraints to conduct interoperability testing. If not the actual agency to perform testing, JITC must still be involved in the planning and execution of the applicable interoperability portions of the Test Evaluation Master Plan (TEMP). This will insure the required information is obtained for JITC to prepare its certification report for J-6.

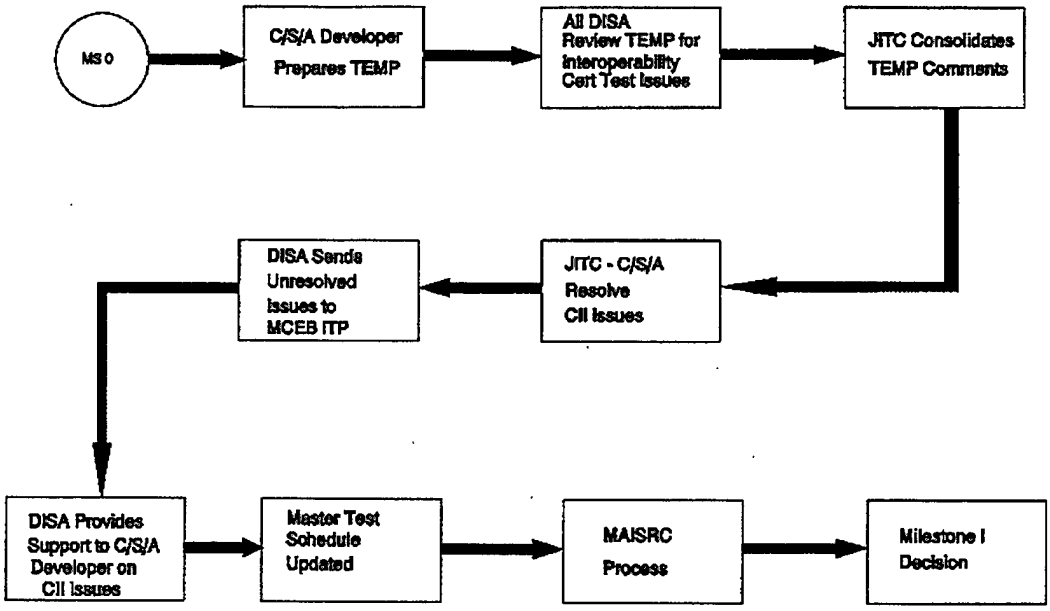

Figure 3-2, TEMP Review Process[21]

2. Test Support

As soon as practicable in the acquisition process JITC should be involved to work with the system proponent in developing an interoperability certification evaluation plan (ICEP) that makes the most efficient use of limited testing assets. The ICEP outlines how the system's interoperability will be evaluated against requirements in the ORD, C4I Support Plan, and TEMP.

---

[21] JIEO/JITC Circular 9002. "Requirements Assessment and Interoperability Certification of C4I and AIS Equipment and Systems". 23 Jan 95.

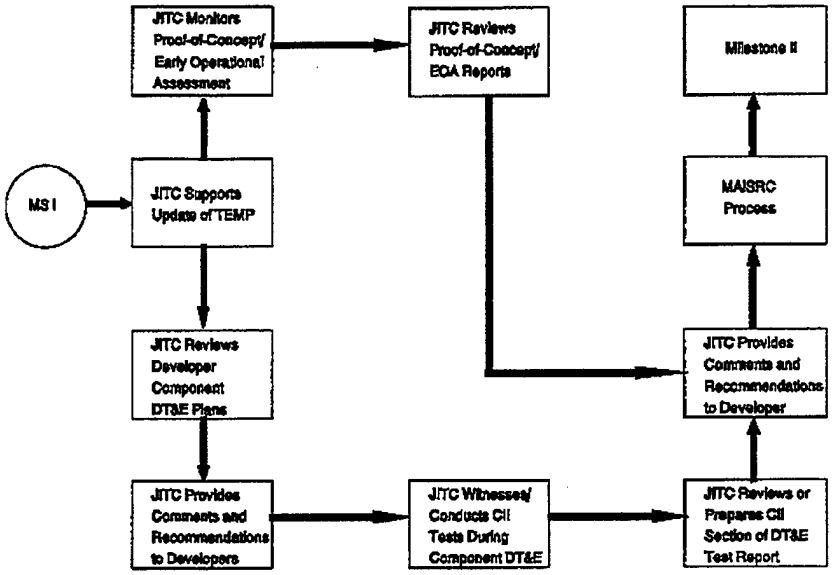

Figure 3-3, Early Test Support[22]

During acquisition lifecycle Phase I (Concept Exploration) CII issues will be addressed utilizing the critical operational issues (COIs) identified in the TEMP. The test methodology to be employed must be designed to test end-to-end CII for the entire SoS. Metrics developed for each interoperability COI must be stated in the ICEP, as well as evaluation criteria and data requirements clearly defined. JITC will work with the Component/Service/Agency (C/S/A) to ensure criteria are translated into testable items. If a COI is not adequately addressed in the TEMP, the certification report to J-6 will state what limitations caused the COI not to be resolved.

---

22 JIEO/JITC Circular 9002. "Requirements Assessment and Interoperability Certification of C4I and AIS Equipment and Systems". 23 Jan 95.

3. Test Review

Systems that have exhibited interoperability problems may be placed on a special "watch list" overseen by J-6's Interoperability Policy Test Panel (IPTP), via the Joint Requirements Oversight Committee (JROC).

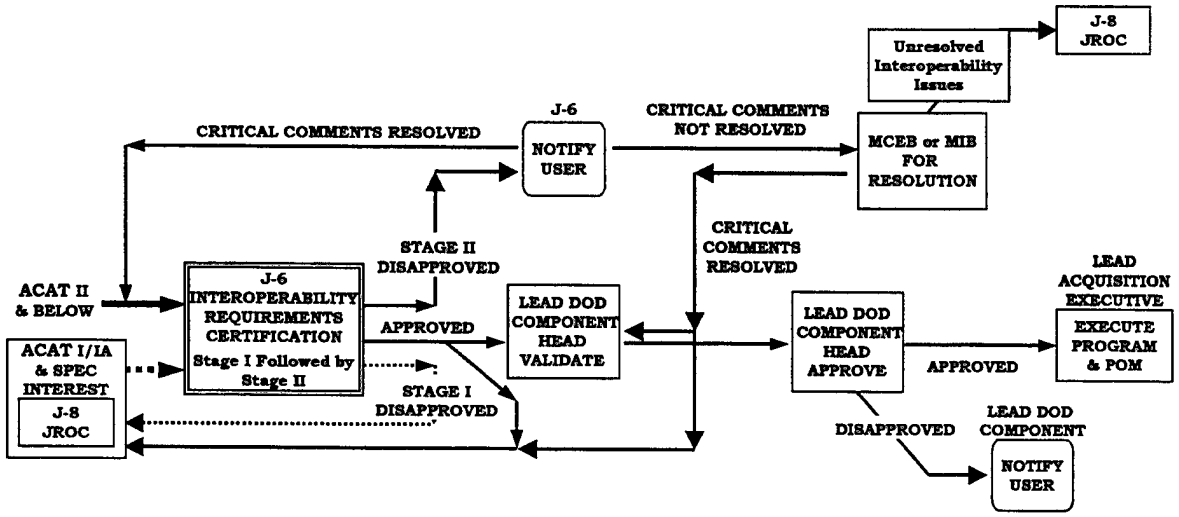

Figure 3-4, Critical Comment Resolution Procedures[23]

The mission of the IPTP is to develop DoD policy positions for Military Communications Electronics Board (MCEB) consideration. The panel acts as the issue resolution forum for interoperability testing and certification matters, to include scheduling, prioritization, and resource conflicts. Additionally, the IPTP is the waiver authority to the certification requirement. A temporary authorization, known as an IATO (Interim Authority to Operate), may be granted in special situations, usually revolving

---

[23] JIEO/JITC Circular 9002. "Requirements Assessment and Interoperability Certification of C4I and AIS Equipment and Systems". 23 Jan 95.

around test resource availability. IATOs are not to exceed one year nor can they be extended or renewed.

In conjunction with the PM for the system that has been placed on the watch list, JITC will provide periodic reviews to the IPTP based upon on-going operational testing of the system's SoS. The IPTP will use these reviews to determine whether adequate progress towards compliance with interoperability test policy and requirements has been achieved in order for the system to be removed from the list. If adequate progress is not achieved or the system is deemed mission-critical, it may be referred to the MCEB for oversight. This is significant in that it empowers the joint constituents in the requirements generation and certification process as well as ensuring the service components do not unilaterally dictate funding decisions regarding interoperability. The MCEB addresses such interoperability issues through two sub-panels. The Interoperability Improvement Panel monitors C4I interoperability issues surfaced by C/S/As, while the Interoperability Test Panel resolves testing disputes, such as appeals of JITC certification decisions.

4. Certification Memorandum

At the conclusion of applicable portions of a system's test program, JITC provides J-6 an interoperability test certification memorandum that is used as input into the acquisition cycle's Milestone III (Production or Fielding/Deployment Approval). The characterization of the memorandum will be based primarily on the performance of the evaluated system's I-KPP. After receipt of JITC system test certification, J-6 will issue a

validation notice to the respective C/S/As and test organizations, as well as forwarding their endorsement of the certification memorandum to the JROC and the appropriate Milestone Decision Authority.

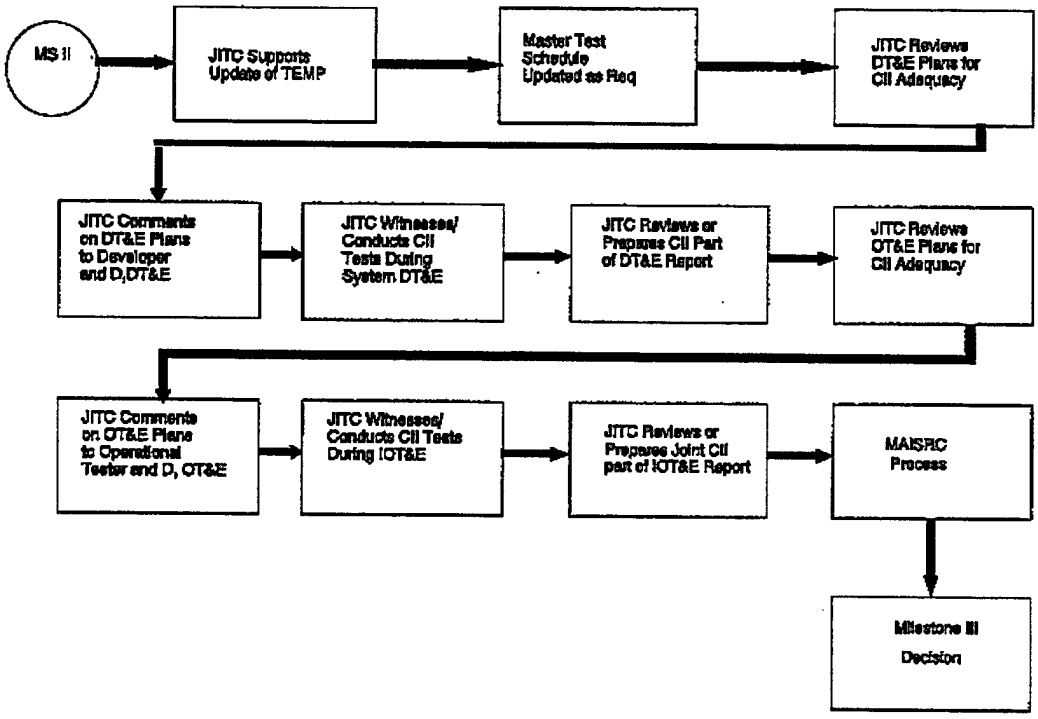

Figure 3-5, JITC Certification[24]

C. CERTIFICATION TESTING ISSUES

1. Introduction

Interoperability certification testing has undergone significant changes since 1999 as a result of the publication of CJCSI 3170.01A. Prior to the "systems of systems" concept, testing was primarily focused on one-to-one interface comparisons and

standardization compliance. With the inclusion of the CRD concept into the requirements generation process, not only was how well an individual element worked with other elements evaluated, but also how well a pre-defined set of CRD SoS elements functioned together to achieve an identifiable mission.

2. US Joint Forces Command

a) Role as Joint Integrator

Due to the increasing importance of joint operations the President's 1993 Unified Action Plan detailed significant changes to the mission and structure of the US Atlantic Command (ACOM). ACOM was given the task of not only serving as CinC for a geographic area of responsibility but to also fulfill the functional areas of providing, training, and integrating all joint forces within the US military structure. Officially re-designated the US Joint Forces Command (JFCOM) in 1999 to better reflect the importance of its new mission, it is the only CinC continuously tasked with providing input to the JROC and the Defense Acquisition Board.

Implicit in this joint integration mandate, JFCOM assumed several responsibilities in the area of interoperability. As executive agent for joint experimentation, JFCOM's observations are critical to the identification of interoperability characteristics necessary to maintain the current qualitative superiority of US forces, achieve the cohesion envisioned in the Joint Vision 2020 strategy, and shape

---

[24] JIEO/JITC Circular 9002. "Requirements Assessment and Interoperability Certification of C4I and AIS Equipment and Systems". 23 Jan 95.

the overarching context for the military of the future. In this capacity JFCOM works closely with C/S/As to identify and refine required capabilities and doctrinal issues. The resulting recommendations often become the basis for conducting joint mission need analyses leading to the development of MNSs (and hence ORDs) and CRDs.

b) Role in Interoperability Process

JFCOM is specifically identified as the CJCS's advocate for joint interoperability. As such, JFCOM provides the "warfighter" perspective during development of joint operational concepts. As a member of the JROC, JFCOM is involved with the formulation of recommendations by the MCEB regarding unresolved interoperability certification issues for developmental and/or fielded systems. JFCOM also coordinates with the Joint Staff J6 and ASD(C3I) who co-chair the Joint Operational Architecture Working Group in the development of the C4ISR Joint Operational Architecture.

As joint force "integrator" JFCOM is tasked with reviewing and confirming the sufficiency of I-KPPs and IER matrices for all ORDs and CRDs. This evaluation is based on the Universal Joint Task List (UJTL) and Joint Mission-Essential Task List (JMETL) assessment process. JFCOM operational testing in support of JITC certification often involves assembling appropriate forces representative of the CRD's SoS in a joint exercise environment. As a result of this redirection of emphasis away from "one-to-one" testing, newly developed metrics used for assessing compliance and

SoS effectiveness now include both mission-based results as well as interface standards compliance inputs.

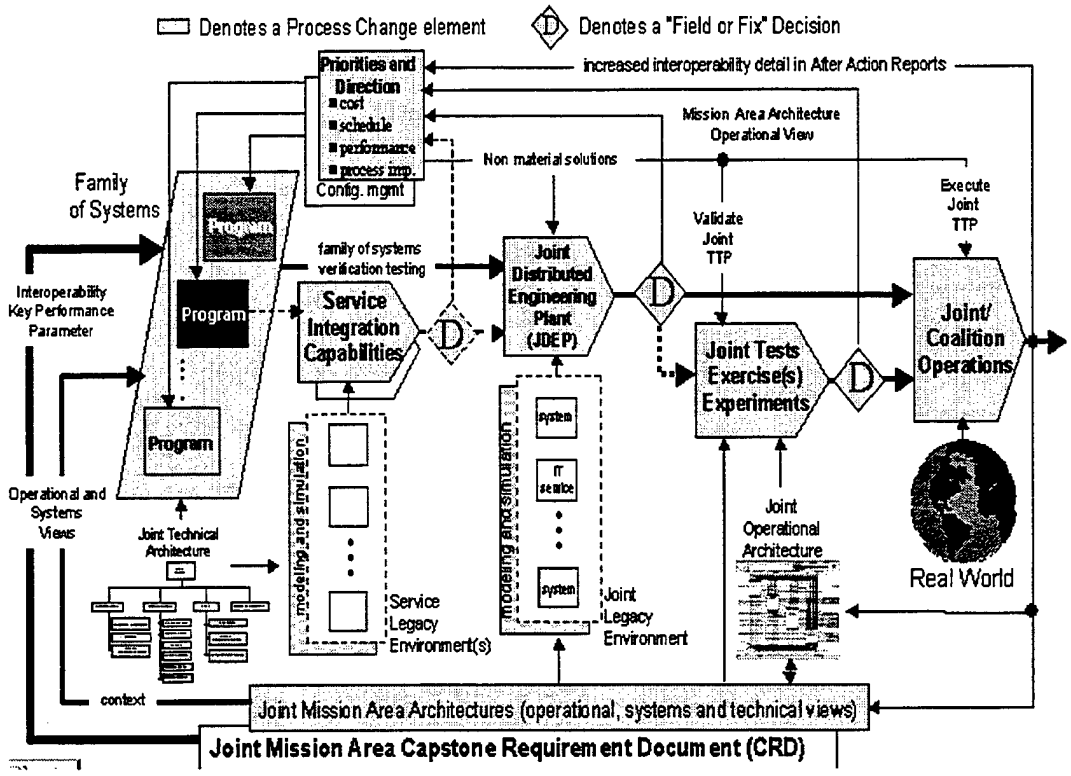

Figure 3-6, Outcome-Based Interoperability Process[25]

c) Joint Command and Control Integration/Interoperability Group

At the suggestion of the Defense Science Board ASD(C3I) established the Joint Command and Control Integration and Interoperability Group (JC2I2G) in November 1998. Two months later the JC2I2G established CinC Interoperability Program Offices (CIPOs) at three different system commands locations:

---

[25] Zavin, Jack, OSD. "Achieving Joint and Combined Interoperability: A Strategic Process". Presentation.

- Communications and Electronics Command (CECOM), Fort Monmouth.
- Space and Naval Warfare Systems Command (SPAWAR), San Diego.
- Electronics Systems Center, Hanscom AFB.

The purpose of the CIPOs is to organize CinC positions regarding interoperability development issues. Along with the CIPOs, a Joint Forces Program Office (JFPO) was also established to provide horizontal integration of the CIPOs' efforts. In addition to focusing on cross-service interoperability, the JFPO is also involved with JTA technical compliance issues.

These organizational entities support JFCOM in its role as joint integrator during the requirements generation process. When faced with assessing interoperability key performance parameters and/or supporting milestone decisions, JFCOM will typically initiate the review process. The cognizant CIPO for the MNS/ORD/CRD being examined will review joint as well as service component requirements. As discussed previously, JITC will assess the testability of the requirements, while the JFPO coordinates CIPO efforts as well as providing reviews of technical requirements.

3. Spiral Development and the Open Systems Approach

The requirements generation system defines the time-phased aspect of the PPBS to support a spiral (evolutionary) developmental approach to acquisition. One of the implications observed in implementing this methodology is that when interoperability is an area of emphasis, an iterative approach becomes more successful than the classic "waterfall" process.

As the CII process progresses, individual system capabilities will often need to be modified repeatedly to better accommodate overall requirements. Spiral development is a streamlined acquisition strategy well suited to automated information systems that seeks to field a core capability based on a modular "open source" design, thus allowing ease of implementation for future increments in capability upgrades.[26]

Open source design is an initiative that began within the commercial software sector that seeks to ensure interoperability among systems procured by different acquisition organizations and developed by different vendors by utilizing common interfaces based on accepted industry standards. Open systems implement sufficient standards for interfaces, services, and supporting formats to enable properly engineered components to be utilized across SoSs with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates *portability*.[27] Open systems are characterized by well-defined non-proprietary interfaces and protocols that have been adopted by recognized standardization organizations as well as the commercial marketplace. Open source design implies that all aspects of a SoS's interfaces have been adequately defined to facilitate inclusion of new, additional, or higher performance system capabilities, a concept also known as *scalability*.

---

[26] Forsberg, Kevin, Mooz, Hal, & Cotterman, Howard. *Visualizing Project Management*. John Wiley & Sons, Inc. 1996.

[27] DoD Architecture Framework Working Group. "DoD Architecture Framework Version 2.1, Volume I: Definitions and Guidelines". 26 Jul 00.

Many current interoperability problems are the result of poor configuration control over systems that were "interoperable" when originally fielded. Interoperability is a constant process throughout a system's total life cycle, a consideration not often accounted for in budgetary and maintenance planning. As this requirement becomes increasingly recognized and accepted it provides another reason for information system acquisition strategies to migrate towards the evolutionary spiral-type development cycle, meaning that all requirements, to include interoperability, can have continuous visibility.

4. Interoperability Certification Challenges

A potential danger exists in becoming too focused on interoperability for interoperability's sake. Arguably, universal interoperability is prohibitively expensive, in time, effort, and technological capability. The so-called "80% solution" can be effectively applied to interoperability, but only when the requirements generation and CRD definition processes provide a valid foundation to adequately frame interoperability trade-off decisions (i.e. where to divide the 80% and the 20%).

While the certification process has undoubtedly furthered the state of interoperability and the capabilities of C4I systems, "certification" should not be construed as a guarantee. Certification only implies that the system is in compliance with the most current standardization protocols and that its IERs and I-KPPs are congruent with those of its associated CRD SoS. The thrust of the certification effort is still focused on the operational testing of one-to-one interfaces within the identified SoS elements.

After a system receives certification, significant problems not identified during testing can arise during its implementation in the less-controlled operational environment. Often, especially during Joint Task Force scenarios, systems are used in ways not previously envisioned. While a system may receive J-6 certification and be approved for production, it will in all likelihood have not been tested against all systems with which it may eventually interoperate, further illustrating the flaw in "interface-only" approaches to testing. As CRD SoSs continue to evolve and emerge, the continuity of the interoperability requirements initiated during the ORD IER process must also be maintained to complete the needs/requirements/capability cycle and to give certification a relevant foundation.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INTEROPERABILITY TOOLS

> Imagine that your automobile was completely disassembled and laid out on your driveway. All the elements individually would be just as before, all in working order. But you would have no transportation. Transportation, the unique system function, only exists when all the elements are connected together and function as a whole.
>
> Eberhardt Rechtin
> *Systems Architecting: Creating and Building Complex Systems*

A. INTRODUCTION

In the past few years there has been no shortage of rhetoric regarding the virtues of interoperability. Even the doctrinal publication *Joint Vision 2020* calls for renewed emphasis in this area. However, all such good intentions are for naught until we have determined the capabilities of the actual tools required for developing, assessing, and diagnosing interoperable systems. This chapter discusses the most promising of these tools, what they can do, and who should be using them. This examination will present two architectural tools: the Joint C4ISR Architecture Plannning/Analysis System (JCAPS) and the Marine Air-Ground Task Force C4I Systems Technical Architecture and Repository (MSTAR), as well as two assessment tools: the Level of Information Systems Interoperability (LISI) and the Joint Maritime Tool for Interoperability Risk Assessment (JMTIRA).

B. JOINT C4ISR ARCHITECTURE PLANNING/ANALYSIS SYSTEM

1. Introduction

JCAPS is an automated software application designed to support the effort of strategic-level planning and resource management by facilitating the comparison, contrast, and integration of C4ISR architectures. JCAPS utilizes standardized application-level data as well as providing connectivity to other SHADE-compliant architecture data repositories. The JCAPS tool helps replace paper-based documentation with architecture information that can be published, queried, summarized, and most importantly, used to achieve C4ISR integration. The JCAPS database holds a core set of common C4ISR architectural data, providing the user with an interactive, distributed, and networked C4ISR architecture planning tool. This capability will help simplify the migration of legacy architectures into new operational, systems, and technical architectural models. JCAPS will also provide operational users a powerful tool in designing ad-hoc architectures as well as a system configuration management tool. The current release of JCAPS employs the guidance and methodologies found in C4ISR Architecture Framework Version 2.0.[28]

2. JCAPS System Configuration

JCAPS employs a three-tiered client/server architecture, packaged in the following ways:

---

[28] DoD Architecture Framework Working Group. "DoD Architecture Framework Version 2.1, Volume I: Definitions and Guidelines". 26 Jul 00.

- As a software component supporting the presentation tier.
- A software component supporting the server tier.
- A software component supporting a data storage tier.

JCAPS operates on a Windows NT platform and supports the exchange of data between clients and servers using an Oracle *8i* database. This three-tiered architecture will allow JCAPS to operate as a stand-alone or networked application.

JCAPS has the ability to share data through replication. This will allow users to work in JCAPS in a collaborative environment. This is ideal for hot-washes following major exercises or deployments where CINCs can articulate their real world operations to the JCAPS central node. This replication will also allow data sharing with such systems as Linked Operations Intelligence Centers Europe, Battlefield Information Collection and Exploitation Systems, and GCCS.[28]

Presentation Tier
• Interface with the server tier to retrieve and display data. No direct access to the database server is available. • All data edited is buffered and passed on to the server tier.
Server Tier
• Responsible for retrieving all required data to pass on to the presentation tier. • Responsible for retrieving all required data from the presentation tier to pass on to the data storage tier.

[28] JCAPS Homepage, https://extranet.if.afrl.mil/jcaps_extra/

• Contains all the algorithms for the manipulation and processing of data that is application specific, i.e., beyond the realm of what can be performed in a stored procedure.
Data Storage Tier
• The repository for stored procedures in support of the presentation tier and server tier. • Stored procedures will be responsible for all business rules and data access, including insert, update, and delete. This will enforce data integrity and the security access required within JCAPS. • Provides role-based dynamic views for independent read-only access by non-JCAPS front-end tools.

Figure 4-1, JCAPS Three-Tiered Functionality[29]

3. JCAPS Development

The Office of the Assistant Secretary of Defense is developing JCAPS in response to the Information Technology Management Reform Act of 1996 that required agency-wide architecture modeling. The utilization of JCAPS ensures that vertical and horizontal traceability and interoperability exists between and among C4ISR Information Systems and their information exchange requirements. The MNS for JCAPS states: "The need for automated cross-architecture analysis from a common information and knowledge base is required to develop coherent, commonly understood "Go-To-War" capabilities for all echelons and to improve DoD information technology acquisition decisions". The JCAPS prototype is currently being evaluated by major geographic and functional

[29] JCAPS Users Manual, Prototype Version 2.1, 1 August, 2000.

CINCs, along with all primary Components/Services/Agencies (C/S/As). It is expected that the final Version 2.1 will be ready for release in early 2001.[30]

4. Summary

JCAPS integrates a variety of powerful technological resources resulting in a broad range of potential users. These resources include the ability to exchange data in a shared environment over a global network, visual drawing tools, graphical information system mapping technology, and the ability to depict all three architectural views. JCAPS provides DoD planners and operators the ability to rapidly prototype, modify and design real-world architectures in a common environment from a centralized database.

C. MAGTF C4I SYSTEMS TECHNICAL ARCHITECTURE AND REPOSITORY

1. Introduction

In 1998 the Marine Corps Systems Command (MARCORSYSCOM) tasked the C4I Directorate with consolidating Marine Corps Operational, Systems and Technical Architectures into a common data repository that could be updated continuously while serving as the central location for all C4ISR technical and programmic information. Prior to 2000, the Marine Corps relied on static PowerPoint depictions of its operational and systems architectures. There did not exist an automated repository for technical architecture data. Access to operational and system architectures could only be gained

[30] JCAPS Homepage, https://extranet.if.afrl.mil/jcaps_extra/

through the Concepts Division of the Marine Corps Combat Development Command (MCCDC).

In response to this tasking the C4I Directorate began developing MSTAR. Logicon, a subsidiary of Northrop Grumman, is the primary contractor for the MSTAR system (as well as JCAPS). MSTAR will be the Marine Corps' central automated repository for all C4I graphical and schematic architecture depictions. MSTAR has a drill-down capability that allows the user varying levels of granularity in the architectural views. In addition, MSTAR incorporates a suite of drawing tools to assist in maintaining and developing new architectures. MSTAR will also have the ability to assess interoperability by utilizing the embedded LISI Inspector Tool. MSTAR has the capability to link systems in the architecture to their programmatic information via the Command Acquisition Programs System (CAPS). This feature gives users the capability to see cost, schedule and program -specific information of each system in order to enhance the C4I operational planning process.

2. MSTAR System Characteristics

a) MSTAR Processes

Like JCAPS, MSTAR also conforms to the guidelines of the C4ISR Architecture Framework Version 2.0. MARCORSYSCOM's System Engineering and Integration Team's architecture development group has outlined six primary functions for MSTAR:

- **Architecture Development** is done in MSTAR through graphical depictions in the client interface. Updates to these depictions are currently only done by MARCORSYSCOM.

- **Interoperability Engineering** is accomplished primarily through the LISI Inspector Tool that has been embedded into the MSTAR system. This tool can conduct interoperability assessments of both stand-alone systems and operational, system, and technical architecture models.

- **Information Assurance** is accomplished by using the MSTAR repository to track MARCORSYSCOM accreditation of recommended systems.

- **Technology Transition** can be tracked using the LISI tool and MSTAR repository to measure the impact of new systems on various architectures.

- **Joint Liaison** can be accomplished by linking the MSTAR system to other services' C4ISR repositories.

- **Systems Integration** is done similar to technology transition in that LISI and technical information in the repository are used to assess the impact of new systems and facilitate their insertion into current architectures.

b) Physical Characteristics

Again similar to JCAPS, MSTAR is based on a three-tiered client/server architecture running Oracle *8i* in a Windows NT 4.0 operating environment. The Client tier is available through any standard TCP/IP web browser, in both NIPRNET and SIPRNET versions. The Applications tier consists of architectural models supported by two drawing application servers known as Aperture and SmartPicture. Oracle's Developer, Forms, Reports, and ColdFusion servers support database repository functions, including dynamic query and DBMS functionality. The Data tier consists of

the MSTAR repository, LISI operational database, and the LISI "playground" (input) database as well as links to external databases that can be implemented as required.[31]

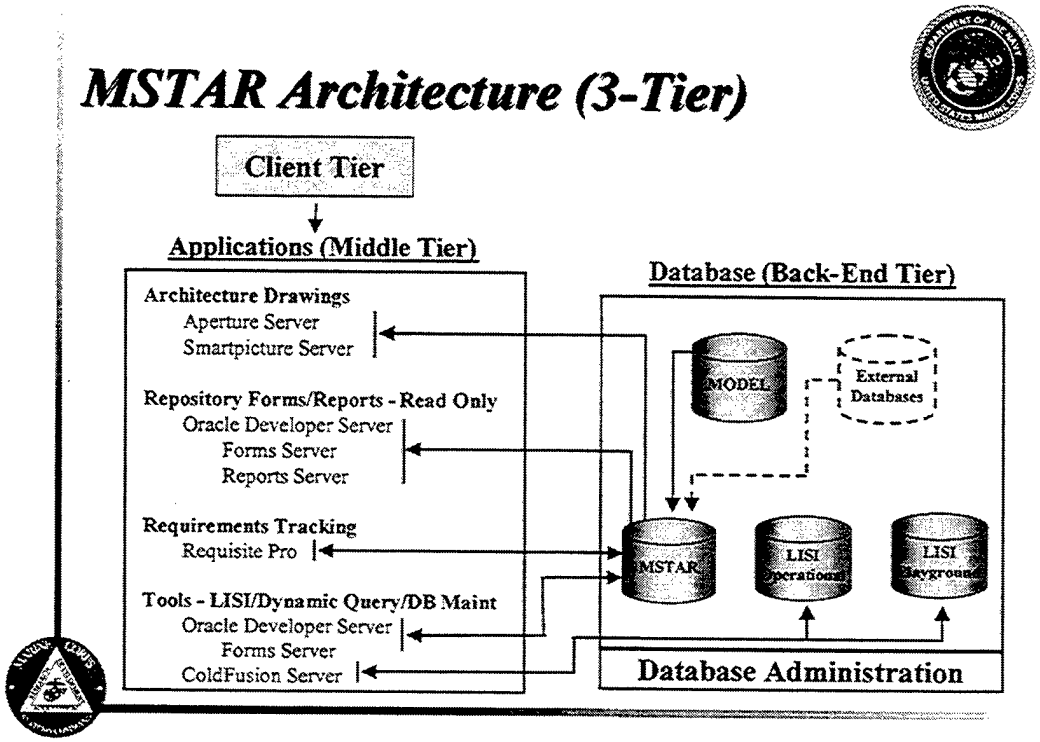

Figure 4-2, MSTAR Three-Tier Architecture.

c) MSTAR Summary

MSTAR is intended to be the central "warehouse" for all Marine Corps C4ISR Architectural Framework information, acquisition development documentation, and individual system interoperability assessments. Concepts Division will continue to coordinate the MNS/ORD process with Requirements Division at MCCDC for all systems that make up the C4I operational architectures of the Marine Corps. The C4ISR

[31] USMC Digitization-C4ISR Near Term Architecture and Efforts Briefing, C4ISR Directorate,

Directorate, MARCORSYSCOM is the keeper of all the systems and technical architectures within the MSTAR repository. Changes to any of the operational, system or technical architectures must be approved by MCCDC and MARCORSYSCOM respectively. Eventually MSTAR will be a tool that warfighters as well as developers will have access to. Initially, operational forces will be able to enter information using the C4ISR Technical Issues forum of MSTAR and the LISI Inspector Tool Questionnaire. MSTAR is a significant step forward in the effort to improve C4ISR system integration and interoperability by C4ISR program developers.

D. LEVELS OF INFORMATION SYSTEM INTEROPERABILITY

1. Introduction

One of the realizations made by DoD was that as an organization it lacked an overarching discipline to recognize different levels of sophistication that logically apply in conducting various system-to-system information exchanges. Such a construct, otherwise known as a "maturity model", would provide the basis for DoD architects to reflect operational differences appropriately, and for MNSs and ORDs to better reflect the desires of the warfighter. LISI was designed to be such a model. Originated by the Intelligence Systems Council in 1993, its scope was significantly expanded in 1996 by the C4ISR Integration Task Force (later handed off to the C4ISR Architecture Working Group). The MITRE Corporation has been the primary industry developer of the LISI model as well as the web-based LISI Inspector Tool.

MARCORSYSCOM, 24 April 2000.

2. LISI Models

The purpose of LISI is to provide DoD with a maturity model and process for determining joint interoperability needs, to assist in the assessment of our information systems in meeting those needs, and in selecting pragmatic solutions and transition paths for achieving higher states of capability and interoperability.

LISI is composed of three different types of models. The LISI Interoperability Maturity Model defines the five levels of system-to-system interoperability in progressive levels of sophistication. The LISI Reference Model characterizes these same levels in terms of four comprehensive and integrated attributes: procedures, applications, infrastructure, and data (PAID). The third model is the LISI Capabilities Model. It defines specific capability thresholds as they relate to PAID in attaining each LISI level. This model provides the detail required in determining system interoperability profiles and metrics, and provides the basic procedural framework for conducting LISI interoperability assessments.[32]

3. Interoperability Capability Maturity Model

The LISI Interoperability CMM identifies and assesses the stages through which systems progress in order to improve their capabilities to interoperate. LISI can then be used as guide for PMs to improve a system's capability to interoperate with other systems or with specific systems called for in a mission-based architecture.

---

[32] Levels of Information System Interoperability Report, C4ISR Architecture Working Group, Department of Defense, 30 March 1998.

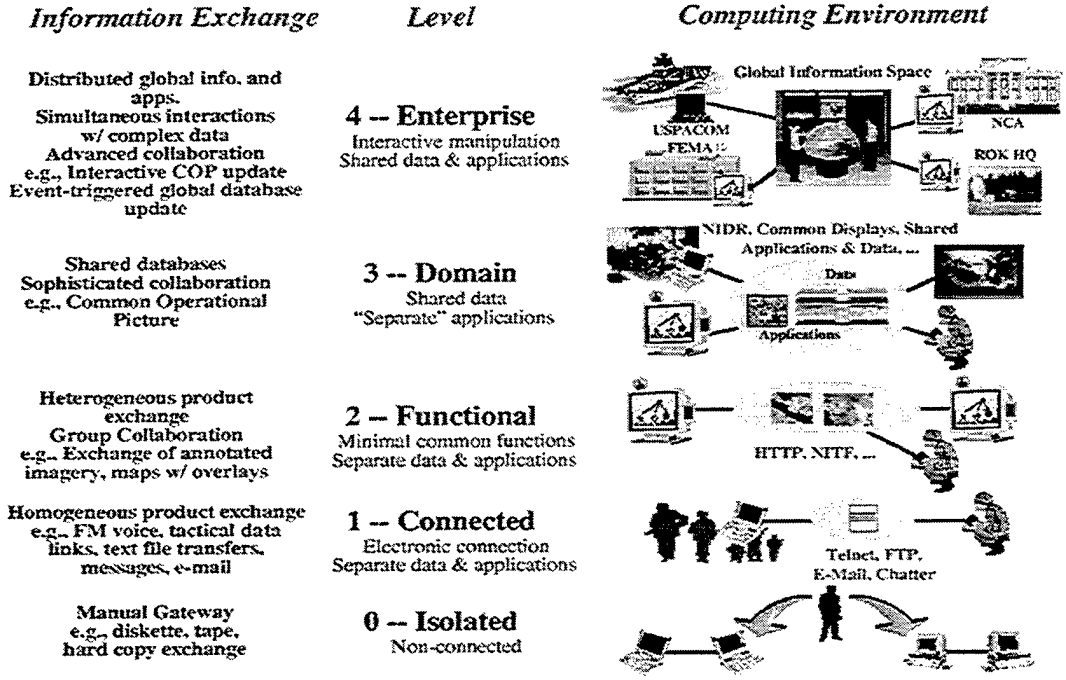

Figure 4-3, LISI Capability Maturity Model

The following provides a brief overview of the characteristics of each CMM level:

- Level 0 (Isolated) generally indicates that a system is stand-alone and either cannot or should not interoperate with other systems (in other words no electronic connection is allowed or is possible).

- Level 1 (Connected) indicates that the system is connected electronically to another system and that they are able to perform some form of simple exchange such as messaging or e-mail. Decision-makers can exchange one-dimensional information but have little capability to fuse information together to support decision-making.

- Level 2 (Functional) indicates that the system is part of a local network with increasingly complex exchanges of information using protocols and some form of formal data model. Decision-makers are able to share fused information between systems of functions.

- Level 3 (Domain) indicates the systems are capable of being connected over a network. Information at this level is shared between independent applications. Domain data models facilitate direct database-to-database interactions. Systems at this level support group collaboration on fused information products.

- Level 4 (Enterprise) indicates that systems are capable of interoperating in a global environment across multiple domains. Data and applications are fully shared and can be distributed throughout to support information fusion. Data has a common interpretation regardless of form, and applies across the entire enterprise.

4. LISI PAID Attributes

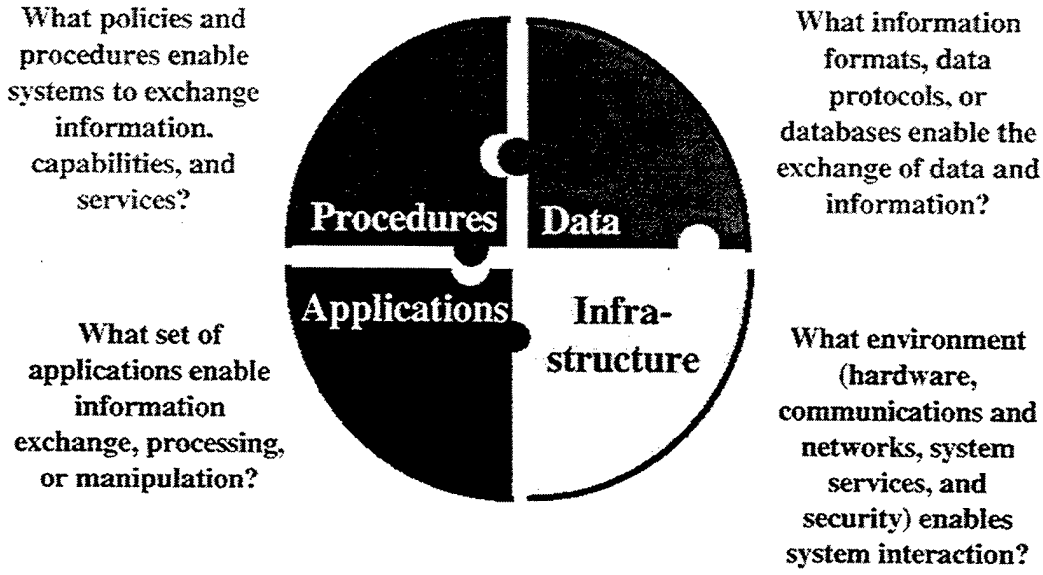

Figure 4-4, PAID Attributes

a) Procedures

The Procedures attribute is broken down into four categories:

- *Standards.* Standards are all the technical standards defined by industry organizations, such as IEEE and ISO, as well as various military standards, such

as the JTA and DII COE.

- *Management.* Management is defined as all aspects of program development, requirements definition, and acquisition/fielding lifecycles.

- *Security.* Security within procedures is addressed as whether or not systems are compatible regarding access. For example, if one system is classified secret and another is classified top secret, these two systems cannot communicate without restriction.

- *Operations.* Operations, as it applies to the procedures attribute, involves the determination by qualified personnel on how systems will be used in accomplishment of the mission.

b) Applications

The applications attribute encompasses the fundamental purpose and function for which any system is built – its mission. The functional requirements specified by users to perform any operational activity are the very essence of the software application. As with the other attributes of interoperability, software applications demonstrate increasing levels of sophistication as they progress upward with the interoperability maturity levels. At the low end, stand-alone applications such as word processors provide a type of discrete functionality. At the mid-range, client-server based applications provide a means for data separation – that is, information is not formatted for use by only a single function; it is accessible in a common format from a commercial database environment. At the higher end, applications are designed for cross discipline or cross-organizational boundaries where common data definitions are required to provide the semantic understanding of the information being shared. Finally, at the highest maturity level of interoperability, the need for duplicate functions and applications is

reduced or eliminated through common understanding and a "system of systems" may now emerge with the ability to function using a global, integrated, information space.

c) Infrastructure

Infrastructure is the attribute that supports the establishment and use of a connection between systems or applications. This connection may be a simple, extremely low-level exchange (e.g., transfer of removable media between systems where no electronic connection actually exists), or it could consist of wireless IP networks, operating at multiple security levels. These examples show the breadth of the communications and hardware aspects represented by infrastructure in the Reference Model. Infrastructure also includes "system services", items that facilitate interactions, such as communication protocol stacks and object request brokers that are used by functions to establish and affect interactions between systems. The security devices and technical capabilities that are used to implement the security elements of the Procedures attribute also make up a part of infrastructure.

d) Data

The data attribute of interoperability focuses on the information processed by the system. This attribute deals with both the format (syntax) and its content (semantics). It includes all the forms of data that support every level of a system's operation. The data attribute embodies the entire range of information styles and formats, to include free text, formatted text, databases, video, sound, imagery, and graphical

information. As such, the data attribute is the most critical aspect of attaining systems interoperability.[33]

5. LISI Reference Model

Description	*Computing Environment*	*Level*	P	A	I	D
Enterprise	Universal	4	Enterprise Level	Interactive	Multi-Dimensional Topologies	Enterprise Model
Domain	Integrated	3	Domain Level	Groupware	World-wide Networks	Domain Model
Functional	Distributed	2	Program Level	Desktop Automation	Local Networks	Program Model
Connected	Peer-to-Peer	1	Local/Site Level	Standard System Drivers	Simple Connection	Local
Isolated	Manual	0	Access Control	N/A	Independent	Private

Figure 4-5, LISI Reference Model

The LISI Reference Model is the foundation of the LISI process. The rows of the LISI Reference Model are the five LISI interoperability levels, the columns representing the four PAID attributes. This matrix provides the broad framework for classifying the degree of capability exhibited by individual information systems. This model also provides the common vocabulary and structure needed to discuss interoperability between

---

[33]Levels of Information System Interoperability Report, C4ISR Architecture Working Group, Department of Defense, 30 March 1998.

systems. Although each PAID attribute must be considered in defining a specific level of interoperability, the significance and relative impact of the contributions from each attribute varies by level. Though attainment of a specific level's capabilities prescribed across PAID is the ultimate goal, one attribute can emerge as a primary enabler for achieving each level of interoperability while the other three attributes tend to provide "supporting" contributions. Understanding the influence between these attributes is critical. The complexity of these relationships illustrates the increasing difficulty of defining the interoperability battlespace. This understanding assists in determining where and how critical resources can be applied to improve future C4I systems development, procurement, and employment.

a) LISI Level-0

The primary enabler of Level–0 interoperability is *Procedures*. Procedures must exist to permit interaction between disparate systems, usually via human interface. Applications do not come into play at this level. Infrastructure is largely independent systems with no connectivity other than physically transportable media, such as 1.44 floppy or Zip disks. Data is typically organized independently with unknown commonalties.

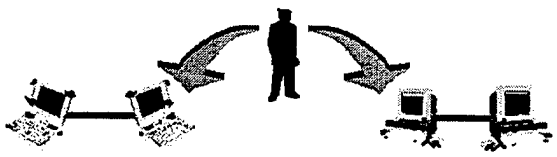

Figure 4-6, Isolated Interoperability in a Manual Environment

b) LISI Level-1

The primary enabler of Level-1 interoperability is *Infrastructure*. Infrastructure provides the physical link between the systems that allows data to flow from one system to another, typically via an electronic connection. This does not necessarily mean that the two systems will be able to exchange information, primarily because protocols at this level of interoperability are extremely low level. The Procedures attribute is characterized by local and site -level procedures. Applications at this level commonly relate to the simple exchange of information electronically. The Data attribute is generally restricted to simple homogeneous data product formats.

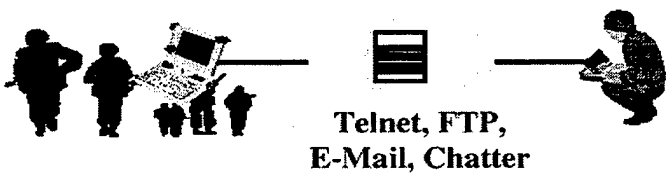

Figure 4-7, Connected Interoperability in a Peer-to-Peer Environment

c) LISI Level-2

The primary enabler at this level is *Applications*. Programs are able to effectively process the information exchanged. Message formats, office suites, and web browsers are examples of this type of interoperability, with TCP/IP and other advanced protocols being introduced at this level. Level-2 is the lowest level that is considered to be DII COE compliant. Infrastructure at this level makes the transition from peer-to-peer to many-to-many connections. Data is characterized by duplicate sub-domain databases

containing heterogeneous information, utilizing metadata definitions and conversion protocols such as ODBC.

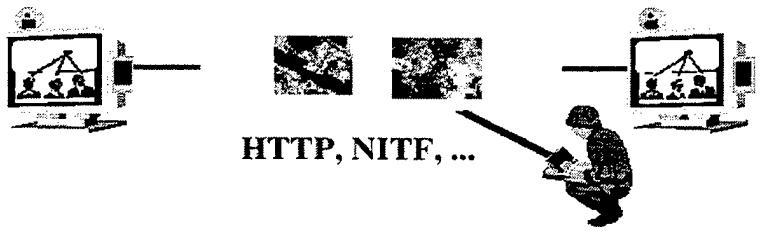

Figure 4-8, Functional Interoperability in a Distributed Environment

d) LISI Level-3

The primary enabler of Level-3 interoperability is *Data*. The Data attribute at this level directs the use of shared databases without data translation, re-mapping, or duplication within a function. Common data definitions, XML and related technologies, and functional/physical data models enable this capability. Procedures at this level are characterized by how well a system conforms to domain-based mission doctrine. This is an area where conflict in the joint environment can occur and is often the most difficult barrier to interoperability while having little to do with the other PAID attributes. Applications that support group collaboration and shared data are present at this level, focused on integration either across organizational or doctrinally defined boundaries. The Infrastructure attribute at this level displays the ability to transition from a LAN to a WAN environment. A domain model that allows direct database exchanges characterizes the Data attribute at this level. This level is comprised of domain-defined data models, dictionaries and standard data elements. Level-3 data is consolidated into shared assets that are correlated and loosely fused, or integrated, by using middle-ware.

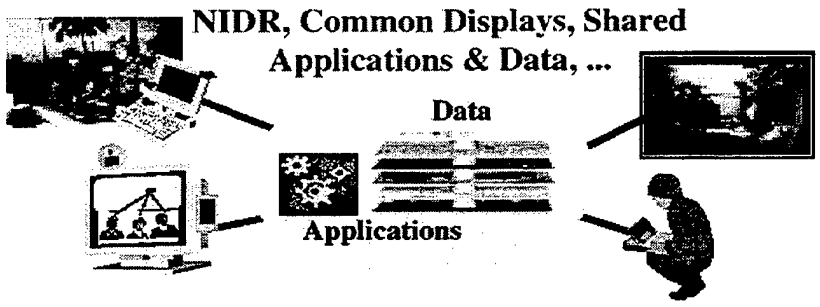

Figure 4-9, Domain Interoperability in an Integrated Environment

e) LISI Level-4

The primary enabler of Level-4 has cycled back around to *Procedures.* Agreements must first be reached on enterprise-wide functions, activities, and operational procedures that cross domain-level doctrine and definitions to ultimately allow universal interoperability. To assess how well a system meets Level-4 requirements is to look at systems documentation (MNS, CRD, and ORD) for the degree of "jointness" to which the system will act across boundaries. Applications at this level are focused on the elimination of duplicative functions and redundant applications via object-level software and component-based architectures. Infrastructure becomes multi-dimensional, advancing over the standard WAN structure by utilizing such techniques as Point-to-Point Tunneling Protocol, protocol wrapping, and Quality of Service mechanisms. An enterprise-wide model that is comprised of universally accepted data models, dictionaries and standard data elements characterizes the Data attribute at this level (i.e. SHADE is fully implemented).[34]

---

[34] Levels of Information System Interoperability Report, C4ISR Architecture Working Group, Department of Defense, 30 March 1998.

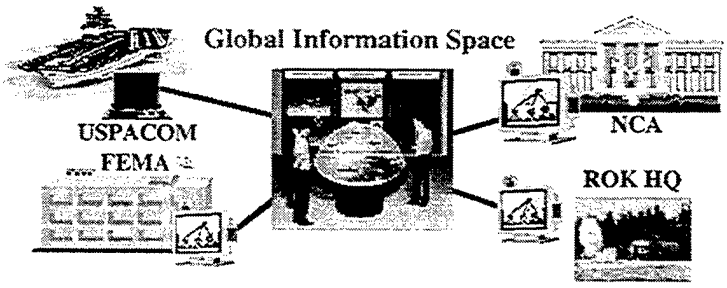

Figure 4-10, Enterprise Interoperability in a Universal Environment

6. The LISI Capabilities Model

LEVEL (Environment)			Interoperability Attributes P	A		D
Enterprise Level (Universal)	4	c	Multi-National Enterprises	Interactive (cross applications)	Multi-Dimensional Topologies	Cross-Enterprise Models
		b	Cross Government Enterprise			
		a	DoD Enterprise	Full Object Cut & Paste		Enterprise Model
Domain Level (Integrated)	3	c	Domain Service/Agency Doctrine, Procedures, Training, etc.	Shared Data (e.g., Situation Displays, Direct DB Exchanges)	WAN	DBMS
		b		Group Collaboration (e.g., White Boards, VTC)		Domain Models
		a		Full Text Cut & Paste		
Functional Level (Distributed)	2	c	Common Operating Environment (e.g., DII-COE Level 5) Compliance	Web Browser	LAN	Program Models & Advanced Data Formats
		b		Basic Operations Documents, Briefings, Pictures & Maps, Spreadsheets, Databases		
		a	Program Standard Procedures, Training, etc.	Adv. Messaging Message Parsers, E-Mail w/Attachments	NET	
Connected Level (Peer-to-Peer)	1	d	Standards Compliant (e.g., JTA)	Basic Messaging (e.g., Unformatted Text, E-mail w/o attachments)	Two Way	Basic Data Formats
		c		Data File Transfer		
		b	Security Profile	Simple Interaction (e.g., Telemetry, Remote Access, Text Chatter, Voice, Fax)		
		a			One Way	
Isolated Level (Manual)	0	d	Media Exchange Procedures	N/A	Removable Media	Media Formats
		c	Manual Access Controls: NATO Level 3		Manual Re-entry	Private Data
		b	NATO Level 2			
		a	NATO Level 1			
		0	NO KNOWN INTEROPERABILITY			

Figure 4-11, LISI Capabilities Model

The LISI Capabilities Model further decomposes the Reference Model to provide a more quantitative assessment of interoperability. As technology evolves the LISI Capabilities Model will evolve also. The LISI 97 Capabilities Model is based on the state of technology and conservative projections as of 1997, and defines the specific thresholds required for attaining each level of interoperability.

What distinguishes this model from the LISI Reference Model is the establishment of sub-levels. For example, the applications attribute displays three specific sub-level thresholds: systems at Level 1a and Level 1b provide simple access or limited-exchange interactions; systems at Level 1c support limited data transfers; and systems at Level 1d provide basic messaging. All of these capabilities represent basic, connected Level-1 interoperability, showing a distinct progression in sophistication and capabilities present within the Connected Peer-to-Peer level for applications.

7. LISI Threshold Rules

The idea of thresholds is vital to how a LISI level is stated. In order to be assessed at a certain level, systems must fulfill all of the requirements identified within the PAID attributes up to the level attained. In effect, the LISI level attained by a system is the "highest line" across PAID up to which all of the requisite PAID capabilities have been implemented and whose implementations have been assessed as interoperable.

Decisions about which thresholds within each attribute are essential or can be treated as inherited are embodied within a rules table. The conditions captured within this table are the reflection of asserting two basic rules:

- Threshold Rule 1: Within the capabilities model, there are explicit, essential capabilities that every system must possess. These capabilities act as barriers to being rated at a higher level until they are accomplished.

- Threshold Rule 2: Within the capabilities model, thresholds are considered as being "credited" to the next higher level if they have not been designated as an essential, required capability as defined in Rule 1.

Essentially these threshold rules determine that a system cannot be rated Level 2a until all attributes of PAID have met the criteria that level; thus if the procedures attribute is Level 1c, the highest overall rating the system can receive is also Level 1c.

8. Applying the LISI Capability Model

The LISI Capabilities Model provides the basis for assessing and comparing systems. Using the model described above as a reference, the individual attributes and capabilities of a system can be captured. Recording these attributes generates Interoperability Profiles for each assessed system or application. In effect, this creates a system-unique profile that shows only those capabilities that a particular system possesses across PAID.

There are three characterization metrics used to express the interoperability level of information systems: Generic, Expected, and Specific. The Generic level of interoperability is the highest level at which the full suite of capabilities is implemented in a given system. The Expected level of interoperability is determined by theoretically comparing (via the Inspector tool) the Generic levels of any two systems. The Specific level of interoperability is determined by comparing each system's specific implementation choices, as exhibited during the actually test and evaluation process. The

Specific level observed may be lower, equal to, or higher than the Expected level. In summary, Generic and Expected levels are obtained by comparing capabilities, while Specific levels are determined by comparing implementation choices.

9. LISI Inspector

Inspector is a tool for capturing, manipulating, and analyzing information system characteristics in context with any coordinate-based reference model, such as the LISI Capabilities Model, DII COE Runtime Environment Compliance Levels, or ISO Protocol Stacks.[35] The Inspector database receives input via system survey questionnaires, typically initiated and maintained by the individual Program Offices. Pre-defined query reports include:

- Generic Interoperability Profile (single system).
- Specific Interoperability Assessment Matrix (system-to-system).
- Composite Interoperability Assessment Matrix (multiple systems – ad hoc configurations).
- System Interconnection Tables.
- Interoperability Attribute Comparison Tables.

The combination of the LISI model and the web-based functionality of the Inspector tool shows promise in assisting in both the development and employment of information system interoperability. However, its potential has yet to be realized due to

---

[35] DoD Architecture Framework Working Group. "DoD Architecture Framework Version 2.1, Volume I: Definitions and Guidelines". 26 Jul 00.

lack of guidance and acceptance on the part of the PMs who are responsible for populating its database.

E. JOINT MARITIME TOOL FOR INTEROPERABILITY RISK ASSESSMENT

1. Purpose and Scope

One of the benefits of the Y2K crisis was the extensive testing of information systems. While Y2K compliance was of paramount concern, it also provided the opportunity for a more overarching assessment of DoD C4ISR systems in general, and several new tools were developed for Y2K testing that can be used in the interoperability effort. One of these tools is the Joint Maritime Tool for Interoperability Risk Assessment (JMTIRA), developed by SPAWAR Charleston. Originally designed as a group of application metrics used to conduct Y2K end-to-end (E-to-E) risk assessment testing, SPAWAR has been tasked with further developing it as a tool for measuring risk in C4ISR systems interoperability

JMTIRA is based on the concept of "emergence". In the study of complex systems, the idea of emergence is used to indicate the arising of patterns, structures, or properties that do not seem adequately explained by referring only to the system's pre-existing components and their interaction. In other words, a systems rather than piecemeal approach will be required to assess interoperability risk factors by reducing the associated uncertainty for architects as well as warfighters.[36]

---

[36] Joint Maritime Tool for Interoperability Risk Assessment Brief to Naval Postgraduate School by SPAWAR Charleston SC, 25 May 2000.

2. Interoperability Risk Assessment

The primary purpose of a fully mature JMTIRA tool is to provide a commander with a risk assessment of C4ISR system interoperability, identifying what potential interconnections may require additional attention and end-to-end testing prior to SoS-wide employment, which can often be complex, time-consuming, and expensive to conduct. JMTIRA has the capability to identify potential system weaknesses, such as network bottlenecks, bandwidth limitations, protocol conflicts, and single points of failure. By identifying high-risk areas prior to joint task force formation, CII efforts can be focused on these areas to mitigate potential problems. Even if highlighted conflict areas cannot be resolved, this knowledge is still vitally important to the warfighter as part of Courses of Action and force protection development.

JMTIRA will typically consider three primary risk factors: System Inheritance, Interface Testability, and Criticality. System Inheritance is the risk associated with the inherent engineering characteristics of a system. Interface Testability is the risk associated with being able to effectively test the system in a controlled integration environment, and Criticality is the mission-based consequence to the JTF if the system does fail.

3. Summary

JMTIRA is still more theory than tool in its current state. However, its underlying Y2K testing methodology has shown promise in being adapted to evaluating

interoperability. To be useful in this regard, JMTIRA will need to develop the following capabilities:

- System /sub-system reliability/maintainability statistics.
- E-to-E system testing results and performance metrics.
- E-to-E system interface interactions.
- System-function mission relationships.

Ideally, the JMTIRA risk factor rating capability would be incorporated into a JCAPS or MSTAR –like tool to provide a complementary (and currently unavailable) functionality.

4. Other Available Tools

a) InterPro

InterPro is an interoperability tool developed especially for the Joint Theater Air and Missile Defense Organization (JTAMDO). It is a SIPRNET tool designed to analyze requirements necessary for inter-system/inter-service compatibility and interoperability within the Ballistic Missile Defense CRD. It has the ability to retrieve detailed data on Service-centric C4I systems but is limited in the same way other tools are by the limited amount of data currently available. It supports Information Exchange Requirement (IER) analysis and provides some automated interoperability analysis functionality. InterPro can create or modify C4I architectures in real-time through an specially designed update interface. Joint testing, exercise assessments, and

combined C4I theater interfaces are being incorporated into its repository at the JITC. InterPro was not assessed in this thesis due to its classified nature.[37]

b) JIT

The Joint Interoperability Tool (JIT) is available through the JITC web site. The JIT is basically a large search and retrieval document-based repository for interoperability related information. A search function allows users (primarily PMs) to research a variety of interoperability topics. JIT features include:

- NATO Interface Guide-allows users to seek guidance on configuring systems to be compatible with NATO countries.
- DoD Interoperability Communications Exercise – gives the user detailed reports and test reports on specific exercises.
- Lessons Learned Reports – provides the user relevant information regarding interoperability lessons learned.
- Certification Summaries – Provides the user completing listing of JITC certifications since FY96.
- Interoperability Test Reports – provides the user JITC Interoperability test reports on selected systems.
- References – the user can view and download instructions and directives related to interoperability.

5. Summary

We have reviewed what we believe to be the most promising tools for constructing assessing and analyzing joint interoperability tools. There may be other

---

[37] http://jitc.fhu.disa.mil

methodologies and tools being used by agencies inside and outside DoD that we are unaware of. What we are certain of is that the tools we have discussed have some of the capabilities required to address C4ISR systems interoperability. In the next chapter we present a more thorough discussion of the capabilities and limitations of these tools.

V. ASSESSMENT OF THE INTEROPERABILITY TOOLS

> I see you've constructed a new light saber. Your skills are complete. Indeed you are as powerful as the Emperor has foreseen.
>
> Darth Vader
> Star Wars Episode VI

A. INTRODUCTION

Despite some of the rhetoric, interoperability among DoD C4ISR systems is not an unreachable goal. Chapters II and III introduced the ambiguity that exists in DoD's policy towards interoperability, but the PM developing C4ISR systems can achieve interoperable system and technical architectures despite the political and bureaucratic jungle before him. A methodology to assist in accomplishing this at the PM level is being developed at the Marine Corps Systems Command (MARCORYSCOM). The goal is to baseline the Marine Corps' "go-to-war" architectures.

Using assessment tools, system metrics, and past test results MARCORSYSCOM wants to be able to give Marine Air-Ground Task Force (MAGTF) Commanders confidence in their C4ISR systems by developing and accrediting operational C4I architectures. In this chapter we discuss how the C4ISR Directorate of MARCORSYSCOM can effectively approach interoperability. This involves a "hands-on" assessment of MSTAR. We look at an architecture constructed in MSTAR called a MAGTF Integrated Package (MIP) and assess the interoperability of this architecture using the LISI Inspector Tool that is integrated with MSTAR. By way of comparison, we look at the same MIP using the JCAPS tool. By conducting this type of side-by-side

assessment we can ascertain the capabilities of two automated tools designed to help PMs field interoperable systems within the C4ISR Architectural Framework and in keeping with the requirements of DII COE.

B. MAGTF C4ISR INTEGRATED PACKAGE

1. Introduction

MIPs are the baseline for near-term and future technical architectures. The MIP depicts the entire technical architecture of a MAGTF. The MIP technical architecture depicts all C4I systems in the Marine Corps inventory and systems that will be introduced into the inventory through the acquisition cycle. Elements in the MAGTF can depicted down to the individual squad level. These depictions represent the Ground Combat Element (GCE), Air Combat Element (ACE) and Combat Service Support Element (CSSE) of the MAGTF. The MIP is an evolutionary product; MARCORYSCOM has designated six MIP levels, each level representing an increase in capability and interoperability. MARCORSYSCOM is currently developing MIP-0, defined as the minimum baseline architecture representing the MAGTF's current C4I systems connectivity. MIPs 1-4 represent progressively more integrated and capable levels to be introduced annually, leading to MIP-5 in FY-05 that represents the fully functional interoperability defined in DII COE.

2. The MIP Levels

a) MIP-0

This level is the current *baseline* architecture that exists in the Fleet Marine Force today. MIP-0 consists of all C4ISR systems currently in the inventory. As of July 00, the MSTAR data repository had architectures for all GCE systems, 60% of CSSE systems, and about 10% of ACE systems. All C4ISR systems had been entered into the database but graphical architecture depictions for the ACE and CSSE elements are not yet fully completed. MIP-0 is a baseline that assumes an environment of limited interoperability because of legacy systems, protocol conflicts, and service-related standards and doctrinal disparities.

b) MIP-1

MIP-1 is the first evolutionary step towards a globally interoperable MAGTF C4ISR environment. It incorporates limited interoperability with US Army systems, includes smaller, more capable hardware/software platforms, and satellite communication integration.

c) MIP-2

MIP-2 begins the movement towards the DII COE's Common Tactical Picture (CTP). Goals of MIP-2 include advanced communication technologies, reduced training requirements, and fusion of maneuver, intelligence and fire support systems.

d) MIP-3

MIP-3 encompasses the fully integrated GCE Unit Operations Center concept that includes wireless LAN technologies as well as a data gateway that integrates the CTP into lower-level C4I systems.

e) MIP-4

MIP-4 encompasses a homogenous software suite residing on a scaleable hardware framework. This architecture would exhibit self-healing and self-organizing capability in its networks, integration of fully functional CSSE logistics capability, and a fused air/ground Common Operational Picture.

f) MIP-5

MIP-5 is the goal of interoperability; completely DII COE compliant, utilizing enhanced technologies such as the Joint Tactical Radio System and Global Information Grid.

3. Developing a MIP

There are two evolutions in MIP development. The first is the MIP specification. Specification is what we want the MIP to be above and beyond the previous MIP level. The second evolution is MIP design. MIP design takes into account the all the changes that the specification will undergo during the MIP upcoming specification and approval process.

a) MIP Specification

The MIP specification starts by examining the following requirements groups: User, System, Function, and Security. These requirements are based on various documents; for example, user requirements come from ORDs, functional requirements from CRDs, etc. Security requirements may have been incorporated into the ORD but can also come from DoD or Executive Policy. System requirements are technical specifications and standards required by DII COE, JTA, or other Marine Corps/DoD standards. The requirements are grouped into sets using the MIP baseline and acquisition programmatic information. Any dependencies among the requirement sets can also be examined at this point.

All requirement sets are prioritized based on guidance from the Management Configuration Control Board (MCCB) and the priorities of the Operating Forces. Metrics are used to prioritize the requirement sets, to include the number of capability sets completed, number of capability sets improved, number of operational facilities (OPFACs) impacted, number of systems impacted, degree to which automation/ simplicity is improved, and which requirement sets best fulfill key performance parameters (KPPs).

The requirement sets are configured with cost and schedule data to the greatest extent possible. Decisions are now made as to which requirement sets seem most promising. It is at this point that programmatic modeling and simulation tools can be effectively used. Once the finalized requirement sets are decided upon they form the

basis of the MIP specification. The system specification consists of the agreed upon requirement sets, system KPPs, standards requirements, systems impacted, and a set of constraints composed of cost, schedule, and performance requirements.

b) MIP Design

The MIP design transforms the MIP specification into a usable document, articulated into operational, system, and technical design architectures. The design process starts by integrating the MIP specification with any new guidance received since the completion of the specification along with Marine Corps/Joint-level policy, issues, and standards. Once changes have been incorporated into the specification the initial design can be constructed. This design consists of four major elements: architectural, hardware, software and standards. The architectural may be a graphical or text depiction of the three architectural views. The hardware design will include elements such as physical connectivity between systems (wire/wireless), the systems themselves (radio, switch, workstation), and other hardware-related concerns to address middleware issues. The software design will specify what software will be implemented from database to office suites, and will reach back to address middleware issues as well. The standards design will be one of the most politically sensitive and difficult design areas to resolve because it affects all other designs.

After the initial design options have been broken out, interoperability assessments are conducted to identify and resolve interoperability issues. Once these issues are resolved through refinement, the four designs are integrated into a single

master design. The master design is mapped to the programmatic issues of cost, schedule and performance and a realistic design implementation plan is attached to the final MIP design.

Personnel from Marine Corps Systems Command and MCCDC Concepts Division work together in developing the MIP specification and design. Other agencies that will have involvement during this process are:

- AC/S C4I, Headquarters Marine Corps (Policy)
- Programs and Resources, Headquarters Marine Corps (Funding)
- Material Command, Marine Corps Base, Albany, GA. (Logistics & Fielding)
- Defense Information Systems Agency (DII COE, DISN, GCCS)
- Joint Interoperability Test Center, (Interoperability Testing & Certification)

These agencies will play an even more important role as the MIP design is routed through the approval process. Missing from this list is perhaps the most important participant: the user. It is unrealistic to assume that the operating forces can afford to designate a full-time representative to the MIP design process despite the critical role they have in its implementation. While MCCDC Concepts Division is the designated representative of the user (by policy), issues that they table on the users behalf may be dated or misinterpreted. MARCORSYSCOM hopes to improve user participation with the use of MSTAR.

c) MIP Approval Process

The MIP Approval process begins with MCCB approving the proposed MIP specification. Once the MIP specification is approved, work on the MIP design can begin. The MIP design is then finalized as discussed earlier, and re-submitted to the MCCB for approval. If approval is given, development of the MIP can begin, otherwise the MIP design is recycled for refinement based on the input of the MCCB.

MARCORSYSCOM is responsible for developing a test plan for the MIP design. One of the factors to be considered in developing this plan is the capability of the candidate test facilities. Questions that should be asked are:

- Does the facility have physical capability to assess interoperability and function?
- Does the facility have simulation tools to assess interoperability and function?
- Can the facility verify that all KPPs are met?
- Can the facility verify IERs and identify the need for new IERs between OPFACs?
- Can the OPFACs be physically constructed or simulated?
- Can the facility test using the prescribed metrics in the test plan?

The PM must also consider what KPPs, IERs, and other measures of effectiveness are testable and affordable. The PM must ensure that data collection measures are in place and what type of format the report will use. The MIP design will be configured for testing and submitted to either the Marine Corps Tactical Systems Support Activity (MCTSSA) in Camp Pendleton, CA or the Joint Interoperability Test

Center (JITC) in Ft. Huachuca, AZ. The function of these organizations is to provide test and evaluation (T&E) of C4I systems in a controlled environment. MCTSSA and/or JITC can perform a wide range of T&E tasks. These include:

- Verification of functions
- Validation of Concepts of Employment
- Risk Reduction Efforts through design, performance and interoperability assessments
- Enable Rapid Replication of trouble calls.
- Assess before/after fielding of system modifications
- Facilitate User assessment and acceptability
- Assess systems for proper implementation of standards, protocols and interfaces.

Reviews of test results will determine what fixes to the MIP design are required. Not all fixes may be pursued; it will all come down to what is feasible under cost, schedule, and performance considerations. Once the PM is satisfied with the tested MIP a fielding decision can be made. MARCORSYSCOM is not certain whether the MIP design will be subjected to the normal acquisition process or if a tailored acquisition approach will be pursued.

d) The Approved MIP

It is important to keep in mind that the MIP is an acquisition program. It is a product that will be delivered for real-world use by the Marine Corps. What makes the MIP unique is that this may be the first time a Service has tried to deliver its entire

"go-to-war" architecture as a configured, tested, and integrated product. One thing is for certain, it will represent the first time the Marine Corps has attempted to integrate its 4ISR architecture.

The fielded notional MAGTF Integrated C4I Package is designed to be a viable "go-to-war" architecture incorporating all three operational, system, and technical views. It integrates all elements of the MAGTF, giving a C4I system of systems capable of exchange with land, air, and sea -based platforms. In the near-term, it gives an usable capability to Marine Expeditionary Forces and ultimately delivers a blueprint for the accomplishment of DII COE compliance and the achievement of Joint Vision 2020 goals.

In reality, the MIP faces many challenges. Fiscal, doctrinal, and political barriers will conspire to impede the development of the MIP. The MIP will also require a thorough understanding of C4ISR Architecture Framework Version 2.0 and must be delivered as a functional product to its users despite the shortcomings of C4ISR Architecture Framework. Most importantly, the MIP must be a product that is embraced by the warfighter. This is perhaps the most difficult task of all. The user is always skeptical of systems in "fancy" packaging. If requirements are not articulated, captured, and developed properly in regards to interoperability the user will be left with much of what he has always had in the past: more fancy packaging.

C. DEVELOPING A MIP WITH MSTAR

1. Introduction

In this section we present an imaginary scenario where two clients are designing/refining a MIP using the features of the MSTAR tool. The first client user is the C4I Directorate of MARCORSYSCOM (PM Client), and the other is a Marine Expeditionary Brigade G-6 (MEB Client). In the first illustration, the PM will be using the MSTAR tool as the MIP design process is progressing through the programmatic cycle. In the second, the MEB will have just completed a joint exercise and based on issues in the C4I debriefings wishes to make refinements to a previously defined MIP architecture. These user-based perspectives will be utilized in order to discuss the benefits and shortcomings of the MSTAR tool, and to suggest how it might be improved.

2. Access and Security

All versions of MSTAR will be accessed via a standard web browser. The PM client will access MSTAR through the NIPRNET, the MEB client through the SIPRNET. MARCORSYSCOM wants to control access to MSTAR due to security, document classification, and input validation concerns. Having both classified and unclassified versions of MSTAR will complicate MARCORSYSCOM's management challenge. The necessity of the unclassified version is for the contractors who do not have SIPRNET access, but any information, especially of a technical nature, would be useless to contractors in a unclassified version. The same could be said for the MEB client wanting to make comments. Any comments they make to MSTAR, especially from an operational theater, would have to be considered as classified. One SIPRNET version of

MSTAR with compartmentalized access would make the most sense. Any contractor requiring access should already be pre-qualified, and SIPRNET-only access helps the operational forces control input to MSTAR. Of greater concern to MCCDC and MARCORYSCOM is the possibility of users (primarily operational forces) submitting issues over NIPRNET when they should be classified. Even on SIPRNET, there is concern that compartmentalized issues can still be submitted within the wrong classification (i.e. top-secret issues going over a secret server). To summarize, what MSTAR ultimately needs is a true object-level security model, a capability beyond the current NT implementation.

3. System/Item Reports

The System/Item Reports options can be accessed by the user via the MSTAR home page. Both the MEB client and PM client have access to the information in these reports. For the MEB client the technical data in these reports is somewhat limited. A description of the selected system and its function is available, but in most cases technical specifications such as power, bandwidth, and protocols are missing. It is hard to envision the MEB client wanting only general information on a specific system. Some programmatic information is available such as acquisition objectives, but the MEB client would benefit from more specific information on system procurement programmatics, such as an actual fielding plan giving a more specific data as to when they could expect new systems. For the PM Client, little of the information in the System/Item reports seems to be of value. Fortunately for both PM and MEB Clients, MSTAR will

eventually tie into the MARCORSYSCOM Command Acquisition Program System (CAPS). CAPS provides specific programmatic information, including fielding plans, technical characteristics, acquisition data, and PM/Sponsor PoCs. However, as of this writing, very little of this information was available in CAPS and most of it was outdated. For the System/Item reports to be truly useful to the PM and MEB clients, system information in these reports must have a greater degree of granularity. Given adequate oversight, this problem should resolve as both the MSTAR repository and CAPS databases mature.

4. The Architecture Depictions

The Architecture Depictions feature of the MSTAR tool is what makes the tool unique and beneficial to PM and MEB Clients; unfortunately it is also the feature with the most shortcomings. Architecture Depictions are graphical illustrations of the MAGTF system and technical architectures. This depiction shows the connectivity of various systems to their respective network clouds. Clicking any of the systems in the depiction retrieves System/Item reports. Clicking network clouds retrieves the network's internal architecture, depicting all systems in the cloud and identifying all subscribers connected to it. These depictions loosely fit the definitions for system and technical architectural views as outlined in the C4ISR Architecture Framework depictions in MSTAR, listed by organizational name or OPFAC. MSTAR's ability to drill-down into the architectural depictions defines the OPFACs into finer levels of detail.

OPFACs listed in these reports do not provide any IERs nor does it label Information Elements, whereas the C4ISR Architecture Framework labels connectivity redundant between two OPFACs if they do not have an IER. While connectivity based on widely accepted standards is a vital component in this since all OPFACs on a network are connected via TCP/IP, it would seem obvious that messages should always get where they are going without the necessity for explicitly identifying needlines or IERs between OPFACs. Only Application-level interoperability can be solved with this sort of "hammer & nails" methodologies such as XML, SNMP, SOAP and CORBA/COM/DCOM (assuming the entire system of systems has IP connectivity). More tangible concerns focus on having the dollars to build out the remaining nodes to become IP compliant and other IP-specific issues such as firewalls, varying levels of classified traffic, and Voice IP latency.

Without IERs, planners and ultimately CINCs cannot designate their most important OPFACs and the exchanges required between them at varying operational tempos. OPFACs will certainly have differing bandwidth requirements than others. Some OPFACs may be more important than others based on the information they disseminate or may have to be shutdown temporarily during high operational tempos. OPFACs, if lost, may affect the rest of the network because of their nature as a critical processing node.

IERs help establish what parts of the networks are the keys to a Commander's risk assessment of his network. If a MEB C.O. wants to know if an AV-8B aircraft can talk to

a Light Armored Vehicle, he could not find specific depictions in MSTAR without knowing what systems are inherent to these platforms, as static depictions of these operational scenarios are not available. This makes for difficult planning, briefs, and hot washes where higher architectural views are typically utilized. It may also be necessary to diagnose why two systems that should interoperate are not. Again, without the ability to display a IER matrix such relationships cannot be shown with MSTAR.

For the PM Client this type of operational view may not be of great concern. However, the PM Client is presented with his own set of challenges. First of all, the Aperture tool inherent in the Oracle database cannot be used through a standard web browser. This drawing tool can only be used by MSTAR developers at C4ISR Directorate, MARCORSYSCOM or Concepts Directorate, MCCDC. Changes to architectural constructs must be manually routed to Oracle-trained Logicon programmers. The requirement to "what-if" scenarios is common in the acquisition arena and would be expensive and time consuming in its current state. This same limitation also affects the MEB Client in a similar manner, where it would be of great benefit for a battle staff to construct dynamically changing architectural depictions in a collaborative environment.

5. LISI Inspector Tool

The interoperability profile link will connect both the PM and MEB Clients to one of MSTAR's most valuable features, the LISI Inspector Tool. LISI Inspector is embedded into MSTAR and is capable of drawing data from the MSTAR repository as well as other repositories linked to LISI Inspector. It is important to distinguish that LISI

is a model and the LISI Inspector is simply an automated tool that uses the LISI model. Inspector is essentially an interoperability questionnaire designed to obtain information on a specific system, store this information in a database, and provide advanced reporting functionality based on this data. The questionnaire presents structured questions that list the available choices for each capability/service that can be implemented in an information system. The data generated from the questionnaire is then used to build system interoperability profiles from both a systems maturity perspective and a pair-wise comparison perspective. The questionnaire is comprehensive, consisting of 256 questions on the characteristics of the system in question. The LISI Inspector tool is designed to generate many of the interoperability assessment products directly from the questionnaire. Both the MEB and PM Clients have full access to LISI capabilities; however, updating information on a system through LISI Inspector is restricted to password authenticated authorized users.

6. C4ISR Technical Issues Forum

This feature (yet to be implemented) will allow the PM and MEB clients to view, edit, or add comments on various C4ISR systems in the Marine Corps and DOD. The feature is fairly user friendly but all entries are limited to text. The tool currently allows searching the repository for specific issues by function, topic, keyword, or system. The C4ISR Technical Issues feature has its own database, so Client's unrestricted write ability does not affect the MSTAR Architecture Depictions or the System/Item Reports.

For both the PM and MEB clients the ability to enter information in formats besides text would be of benefit. Technical data, schematics, depictions, presentations and even pictures should all be formats that should be accepted by the MSTAR system. Because this forum does not affect the MSTAR baseline data, this could be one of the avenues to incorporate drawing capabilities and in time this could become the most useful feature of MSTAR. By utilizing the available Oracle client collaboration tools this could also become an engaging forum for operational planners and program developers.

7. Summary

MSTAR is not yet ready for "prime time". Significant work remains in populating the database and more detailed technical information is required in the System/Item reports. The ACE and CSSE elements will still need to be completed in the MSTAR architectural depictions. The tool does not really present an operational view as defined in the C4ISR Architecture Framework. The most serious shortcoming is the inability for a client to modify architectural depictions or technical information directly. This deficiency inhibits operational planning and "what-if" scenario construction. The MEB client cannot realistically make design changes to a MIP. His only avenue is to make suggestions in text format, limited to 4000 characters. The PM Client, despite being the keeper of some of the systems in the architecture, has the same limitations. The C4I Directorate, who is the "owner" of the MSTAR database, can use Logicon contractors to build/revise architecture depictions or System/Item information, but other PMs who have system specific data to update do not have direct access (providing an

unnecessary level of frustration in a command as contentious as MARCORSYSCOM). The inability of the PM and MEB Client users to make MSTAR inputs without immediate MSTAR feedback will ultimately adversely affect user acceptance. This is unfortunate because the need for a central repository for MAGTF architectures is vital to the overall interoperability effort, but the users must be allowed to affect the process if the architectures are to be credible.

D. DEVELOPING A MIP WITH JCAPS

1. Introduction

Like MSTAR, JCAPS's primary function is the development and presentation of architectures within the guidelines of the DoD C4ISR Architectural Framework. Perhaps the most glaring difference between the two is that the JCAPS program has the backing of OSD while MSTAR is supported solely from within the austere fiscal environment of the Marine Corps. JCAPS Version 2.1 is being evaluated by all theater CINCs and major Unified Commands, while MSTAR is still relatively unknown even in MARCOESYSCOM. JCAPS is still client-server based (unlike MSTAR's web-based implementation) but it can function much more effectively in a collaborative environment, where clients will be able to interactively create and revise architectural depictions. JCAPS does not have an interoperability assessment tool per se but plans to interface with the LISI Inspector tool (much like MSTAR) in future versions.

2. Access & Security

JCAPS must be run over a secure LAN in client-server mode. Eventually JCAPS will be a web-based enterprise server with access via standard web browsers. MEB clients accessing via the Web will be able to create and modify some of the systems data contained within the JCAPS database, while the PM Client will have easier access to JCAPS initially. In either case, access is controlled currently through the OSD JCAPS program office and distributed individually to commands for installation. Once the web-enabled JCAPS enterprise server/database becomes available users will still need client software to run the various drawing tools and features. The "owner" of the JCAPS enterprise server/database (yet to be determined) will administer security.

3. Tools Cabinet

The first feature clients will want to use is the Tools Cabinet. This allows the client access to the fundamental building blocks of JCAPS operations. These Elements will allow the PM and MEB Client to create/revise their MIP depictions. Elements are populated by two different sets of data: world and architecture. World data elements are not associated with a specific architecture already designated in the JCAPS repository, while architecture data are associated with a specific architecture. Either of these sets of elements can be manipulated with the tools cabinet.[38]

The C4ISR Core Architecture Data Model (CADM) defines the Organization element in the tools cabinet. Organizations in JCAPS can encompass everything from

---

[38] JCAPS Hands-On Training Guide (Prototype 2.1) 1 Mar 2000

military organizations and OPFACs all the way up to national governments. In a broad sense, an organization is an operational element, and thus can have Information Exchange Requirements (IERs), or Activities relating to other organizations, but in JCAPS this is reserved exclusively for entities designated as OPFACs. The OPFAC is defined as a specialized Node within JCAPS. Generally, OPFACs are envisioned to be subordinate to organizations. An OPFAC belongs to an echelon of command and performs activities within a particular mission. An OPFAC is an operational element and thus can have IERs or activities relating to other OPFACs.

The Activities Element is associated with OPFACs. The CADM defines an activity as an operation in a process that is designed to accomplish a specific task or set of tasks, while a mission is defined as the task, when together with the purpose, that clearly indicates the action to be taken and the reason therefore. An activity can originate from the Universal Joint Task List (UJTL), an Activity Model, or a user-defined task that supports the mission. In JCAPS, an activity simply describes a process that occurs between two OPFACs, and OPFACs can have multiple activities.

Another feature in JCAPS is known as User Definable Properties. This feature allows a user to "create" new data fields for each element type and then associate a property or name to this new data field. This feature can be used as part of a user defined query. The Tools tab creates User Definable Properties for each element in JCAPS. We found JCAPS to be lacking in Marine Corps specific systems, but with this feature both clients can create and populate systems and in turn, further enhance the JCAPS database.

4. Creating A New Architecture

Creating a new architecture is a two-part process, which includes identifying the new architecture to the JCAPS program (i.e. giving it a unique name) and developing individual products to support it. Currently prototype JCAPS Version 2.1 supports the six C4ISR Architecture Framework products listed below:

Product Reference	Architecture Product
	Operational Products
OV-1	High-level Operational Concept Graphic
OV-2	Operational Node Connectivity Description
OV-3	Operational Information Exchange Matrix
OV-4	Command Relationship Chart
	Systems Products
SV-1	Systems Interface Description
SV-2	Systems Communications Description

Figure 5-1, Framework Products Supported by JCAPS.[39]

The High-level Operational Concept Graphic gives an overarching perspective of the operational scenario. It represents the operational components within the mission landscape and can be used as a means of orienting and focusing detailed decision making,

[39] JCAPS Hands-On Training Guide (Prototype 2.1) 1 Mar 2000

serving as a visual sketchpad for the operational scenario. For MEB Client this is a key feature that MSTAR does not have.

The Command Relationship Chart is a graphical depiction of the hierarchical relationships between operational elements. This is similar to the organizational constructs in MSTAR. Lines of command and control can be drawn among the operational elements. For example, it would be easy using the tool to depict the command relationships for a MEB. The decision making structure of activities between the operational elements can be drawn by designating elements as parents, children, or siblings.

The Operational Node Connectivity Description is a graphical representation of the specific relationship between two or more operational elements. This relationship would be two OPFACs exchanging information elements. The sum of these is an IER and is represented as a needline between two OPFACs.

The Operational Information Exchange Matrix describes the same information has the ONCD only in a tabular rather than graphic form. Similar to a spreadsheet, the columnar headings would have the Information Element, Activity, OPFAC, and Organization. The total number of IERs could easily be computed from this format. This feature is what gives significance to JCAPS operational architectures. More importantly, drawing architectural views in JCAPS is system controlled through this function. For example, if MEB client wishes to draw connectivity between two OPFACs he must have an IER between the two to do it. If he attempts to connect them with a user-defined

needline without an associated IER the program will not allow him to connect them. This type of control ensures that the operational architecture depictions in OV-1 and OV-2 remain valid. This type of functionality is what is missing in MSTAR.

The System Interface Description represents the communication pathways between systems, nodes, and components of a system. A detailed description of the communication pathway or network can be retrieved from the Systems Communications Description, giving specific information of a network pathway or communication link such as bandwidth, data rate, channels, and frequency.

5. Summary

JCAPS is a significantly better C4I architecture construct tool than MSTAR. It allows clients to quickly design "what-if" scenarios in a collaborative environment. As JCAPS matures, all technical views of C4ISR Architecture Framework will be available and JCAPS will be able to show higher degrees of granularity. For example, needlines can be constructed as network connectivity "pipes" indicating bandwidth characteristics, number of subscribers, and what resources can be shared, all characteristics of IP networking.

Unlike MSTAR, JCAPS has all ready undergone a "live-fire" assessment. The Joint Forces Program Office (JFPO) conducted an assessment of JCAPS by capturing and documenting an architecture describing the US Alaskan Command. Based on their assessment, JCAPS is poised to transition from a prototype to an operational system, with the following caveats: SIPRNET accreditation needs to be expedited (done); Network

element support/NETWARS data interchange is critical; and the program office should focus on solidifying existing views vice the addition of new views. The ALCOM effort required the identification and entry of over 2200 unique elements and nearly 60 products were generated to visualize the architecture. As a result of the exercise approximately 75 problem areas were observed (note that this is the point in the process where the JMTIRA risk assessment tool could assess the associated risk level).[40]

E. THE LISI INSPECTOR INTEROPERABILITY ASSESSMENT OF THE MIP

1. Introduction

The LISI Inspector tool is embedded into MSTAR and can draw from the MSTAR repository. The Inspector is also available over the Internet through the CinC Interoperability Program Office (CIPO) at SPAWAR, San Diego. Both the MSTAR repository and the LISI repository at SPAWAR contain the same data for Marine Corps C4I systems. Unfortunately, neither database contained enough data for a thorough evaluation of our notionally constructed MIP. Neither the MSTAR nor JCAPS tool allowed us to completely construct a MIP. Most of the data available in the repository was on systems either recently or yet to be fielded. Legacy systems for the most part simply did not have data populating the repository, owing to the fact that no organizational entity has yet been singly tasked with this responsibility. Some items were not even listed in the database. Of concern here is that our notional architecture was of

[40]Mitre, Corp. "Analysis of JCAPS Live Fire Results" Joint Forces Program Office, 20 Dec 99.

perhaps the simplest of units (an infantry battalion) with a very low C4I sophistication level, and could still not perform a full LISI Interoperability assessment with the tool due primarily to lack of data. This indicates that a significant area of emphasis will be simple data capture/entry if LISI is to be a viable assessment tool for use at the Joint Command level.

2. LISI Products

Before we discuss the specific LISI products that will be produced in this assessment, let's review the Generic, Specific, and Expected levels of interoperability and what they mean. The Generic level is the value of comparing a single system against the LISI Capabilities Model. For example, if a Marine DACT terminal is at Level G4a, only the DACT terminal was assessed against the Capabilities Model. The Expected level is assessed for a pair of systems and is the value assigned against the Capabilities Model but without an implementation-by-implementation comparison between the two systems. For example, comparing DACT (G4a) against AFATDS at G1c it is expected that the two systems will be able to perform interactions characterized by E1c. The Specific level is the value assigned against the Capabilities Model between two systems when specific implementation choices are made. The Specific level may be different than the expected level based on the added use of the LISI Options Tables and the consideration of technical implementation choices. The Specific level for a DACTS/AFATDS comparison may be lower than E1c if the implementation choices made to facilitate a particular capability are not compatible. This is often the case when two systems have

different security constraints. The Specific level for a DACTS/AFATDS comparison can also be higher than E1c if there is an extended interface between the two systems that allows them to interoperate at a level higher than expected. This can be the case with the introduction of software to two systems not documented in the LISI database.[41]

3. LISI Products and MIP Interoperability Results

The LISI Inspector Questionnaire forms the bridge between the LISI Models and the LISI products. PM and MEB Clients will select choices in the questionnaire that will allow LISI Inspector to generate four primary sets of assessment products. The four assessment products are:

- Interoperability Profiles
- Interoperability Assessment Matrices
- Interoperability Comparison Tables
- Interoperability System Interface Description

a) Interoperability Profiles

Interoperability Profiles map LISI Questionnaire data to the LISI Capabilities Model template. In this case we evaluated the MIP systems available in the LISI database and it generated generic Interoperability Profiles for each system. In many instances a G0o ("undefined") was assigned for the MIP systems. For this demonstration we assumed that if the system was listed in the database, then data was available for an

[41] Levels of Information System Interoperability Report, C4ISR Architecture Working Group, Department of Defense, 30 March 1998.

assessment. Appendix 1 gives the Generic interoperability profiles of the systems in our notional MIP that appeared in the LISI database.

b) Interoperability Assessment Matrices

HOME | SEARCH | REPORTS | HELP

LISI Projected Interoperability Assessment Matrix

Unclassified

Systems		AFATDS	AN/MRC-145	AN/FRC-119A,B,C&E	AN/FRC-68A	DACT N/A	GCCS	IAS MSBL 1.1	PLRS COMM (PCE) UNKNOWN	TCO
As of date	Generic Level	1c	0o	0o	0o	4a	3c	3c	0o	3b
AFATDS Aug. 1999	1c	3b	0o	0o More	0o	3b More	3b More	3b	0o	3b More
AN/MRC-145 Aug. 1999	0o	0o	0o	0o More	0o	0o More	0o More	0o	0o	0o More
AN/FRC-119A,B,C&E Aug. 1999	0o	0o More	0o More	0o More	0o More	0o More	0o More	0o More	0o More	0o More
AN/FRC-68A Aug. 1999	0o	0o	0o	0o More	0o	0o More	0o More	0o	0o	0o More
DACT N/A Sep. 1999	4a	3b More	0o More	0o More	0o More	4a More	3c More	3c More	0o More	3b More
GCCS Sep. 1999	3c	3b More	0o More	0o More	0o More	3c More	3c More	3c More	0o More	3b More
IAS MSBL 1.1 Apr. 1999	3c	3b	0o	0o More	0o	3c More	3c More	3c	0o	3b More
PLRS COMM (PCE) UNKNOWN Jan. 1999	0o	0o	0o	0o More	0o	0o More	0o More	0o	0o	0o More
TCO Aug. 1999	3b	3b More	0o More	0o More	0o More	3b More	3b More	3b More	0o More	3b More

No Interoperability Identified | Specific LESS but SAME LEVEL as Expected | Specific GREATER than Expected

Specific LESS than Expected | Specific EQUALS Expected | No requirement to interoperate

Figure 5-2, Interoperability Assessment Matrix

These products interrelated groups of systems based on their Generic, Expected, and Specific interoperability levels. The results are presented in a matrix format that enables each system pair to be compared. This format makes this product useful to both types of clients in systems development, acquisition, and operational planning. In our assessment we used the projected Interoperability Assessment Matrix. This matrix can be generated for a group of systems based on the Generic interoperability level of each system and the Specific interoperability level for each system pair within the group.

c) *Interoperability Comparison Tables*

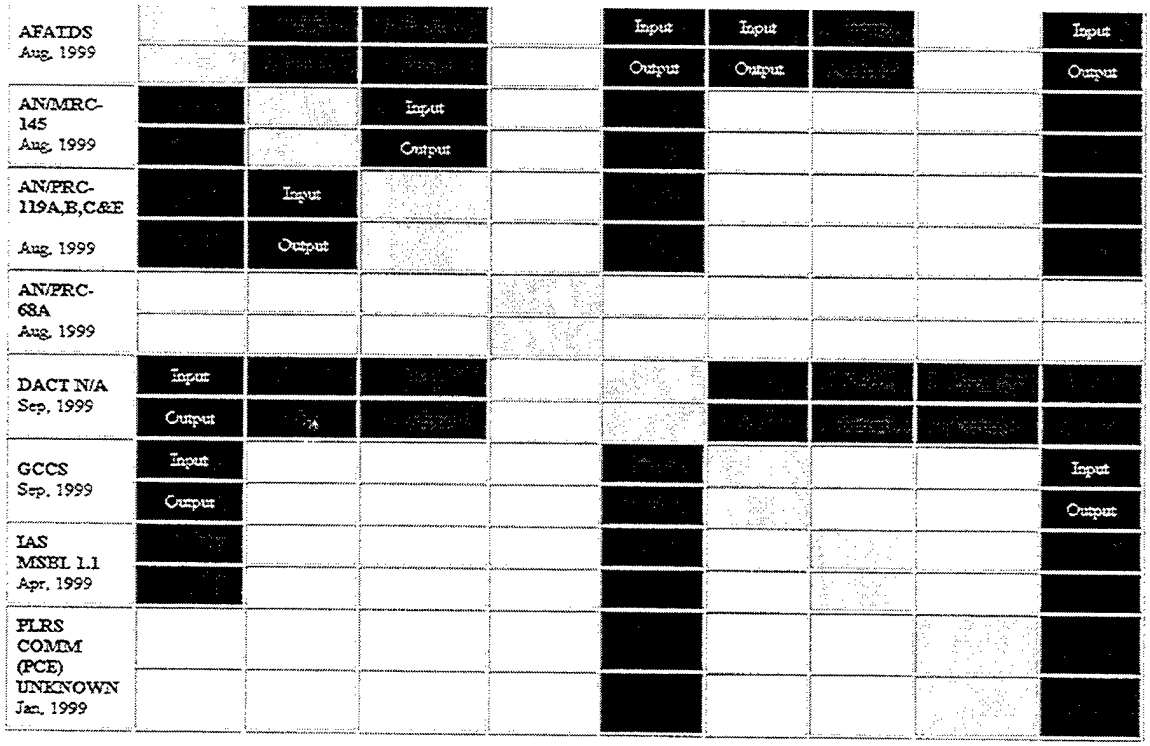

Figure 5-3, Interoperability Requirements Matrix.

These products present the results of system-to-system PAID implementation assessment. These products provide a comparison of interoperability implementation information between systems in terms of PAID. The product we used was the Interconnection Requirements Table. A major factor that drives interoperability relationships and requirements is agreement among organizations and PMs on the need of particular systems to share inputs and outputs with one another. This table takes the LISI questionnaire data that specifies what systems should talk to each other and then lists them as input and outputs with one another. The I/Os are color-coded: green for an agreed upon exchange; red if the exchange is not agreed upon; yellow for a partial agreement; and gray for requirements not expressed by either system. For example, the DACT has an agreed upon information exchange with AFATDS and GCCS but not with IAS, based on information provided by the PMs and entered into the LISI database for each system.

d) Interoperability System Interface Description

As seen previously the C4ISR Architecture Framework defines standard products to describe the operational, systems and technical views and the relationships between them. Information from LISI can be incorporated into many of these products to quantify the interoperability aspects of C4I architectures. Basic information from System Interoperability Profiles can be directly applied to architecture products. For example, LISI can depict the node connectivity of our notional MIP and the interoperability levels it is functioning at between systems. The MEB client may wish to drill down to the

interoperability level between the infantry battalion and another rifle company. As long as the MEB client knows what systems the battalion and company are using and they are in the LISI database, LISI will give a nodal view of the connectivity between the two.

4. The Future of Interoperability Tools

As would be expected, PMs for JCAPS, MSTAR, LISI and JMTIRA all have future development plans for their respective tools. Unfortunately, none of these programs receives much budgetary consideration. While JV2020 explicitly names interoperability as a critical issue, funding decisions continue to not reflect this.

a) JCAPS Future Development

Based upon ongoing DoD evaluation, JCAPS will incorporate user recommendations into a new version currently under development that will include a transition to an three-tiered web-based enterprise approach. JCAPS will also integrate decision support and knowledge management functions (known as the Joint Mission Area Analysis Tool) into its database to further enhance C4I and C2 planning at the operational level. JCAPS 2.1.1 features an interface to other service C4I data repositories, to include the LISI Inspector Tool and LISI Database; however, there is no functionality planned to allow reverse access by outside systems. Lastly, acquisition program information and expansion of its capabilities to more fully support logistics and administration structures are also being planned for JCAPS.

b) MSTAR Future Development

MSTAR plans to develop a more robust operational view depiction that would include the ability to extract General Officer -level presentation capability. It will also extend its integration of acquisition program information to include configuration management tools, work breakdown structures, integrated process team presentations, and requirements documents parsing/categorization. It is clear from these planned efforts that MSTAR will remain primarily a tool for program developers and managers at MARCORSYSCOM.

c) LISI Future Development

LISI and its Inspector Tool are perhaps the most mature of the tools we evaluated. LISI will continue to populate its database and extend integration with other C4I technical databases both in DoD and the commercial sector. LISI will also be adding another level, coined "Unified", to its five layer Capabilities Maturity Model. Inspector will also continue to develop its profile questionnaires to provide even a greater degree of granularity in its report capability. Most importantly, as technology evolves the LISI model is perhaps the most flexible and easily adaptable, and for these reasons may very well remain the most central and relevant of the tools.

d) JMTIRA

JMTIRA is the least evolved of the products we have evaluated, remaining more methodology than tool. JMTIRA will improve the integration of its database to advanced statistical algorithms as well as converting its database structure to C4I system

and technical data to support interoperability vice Y2K risk assessment. JMTIRA will eventually also be incorporated by modeling and simulation efforts such as the Network Warfare Simulation (NETWARS) and the Joint Modeling and Simulation System

F. SUMMARY

The interoperability and integration tools we assessed show considerable promise. PMs and operational planners can take comfort in knowing that automated tools are on their way. All the tools assessed require more development, but integration among the tools is even more critical. Our MIP cannot currently be constructed with the tools in their current state. Given a degree of integration between all the tools examined, a good cup of coffee and a computer with a goodly amount of RAM, we could have constructed our Infantry Battalion MIP in a matter of hours. It is critical for DoD to continue development of these tools. We find it interesting to note that one of the critical factors in making this "system" of disparate interoperability tools fulfill their collective promise is their ultimate ability to interoperate amongst themselves.

VI. CONCLUSION

> Architecture is life, or at least it is life itself taking form and therefore it is the truest record of life as it was lived in the world yesterday, as it is lived today or ever will be lived.
>
> Frank Lloyd Wright

A. INTEROPERABILTY: PAST, PRESENT, AND FUTURE

1. Compatibility to Interoperability to Integration

Thankfully, interoperability has been receiving increased attention from the operational community. As forward-looking doctrinal discussions such as Joint Vision 2020 take place, it is becoming apparent that achieving dominance of the "infosphere" requires much more than just having the most advanced information systems. Returning to Assistant Secretary of the Navy Buchanan's analogy from Chapter II, we know we already grow the best vegetables in the world, and we are slowly, painfully learning which ones taste best with each other. What still remains is to figure out how to put it all together in a salad that someone will actually be able to eat.

Interoperability success in the past has come as a result of the certification effort and the emphasis on standardization compliance. We have realized for some time that the devil of assuring interoperability is in the details of implementation. The problem we continue to have is that testing and evaluation efforts have been predominately focused on System-Centric issues. Certification of system-to-system interfaces does not conclude the integration process; it merely begins it.

Much of today's efforts in development and testing are necessary to deliver functioning individual capabilities. Individual system certification and verification will continue to be required to ensure architectural and standards-based compliance. The process of determining and defining all the elements that make up the continuously evolving DII COE is a full-time endeavor. However, what we are beginning to find is that this effort is only a part of the overall solution. Evaluating individual systems and testing dual-system interfaces is not the same as examining an entire mission-based system of systems. Whereas much of the past's emphasis was on compatibility and today's is on interoperability, the future challenge we must face is **integration**.

2. Mission-based Testing

Today's interoperability testing component is still almost exclusively technically oriented, but more importantly, plays its greatest role late in the development effort as the program nears completion. To take the next step towards the ultimate goal of systems integration, testing in general must not only be focused on standards compliance and system acceptance but must also begin to consider the contribution to mission accomplishment of the individual system *within the context of the SoS*. Interoperability needs to be driven "top-down" by considerations of operational significance (vice simply complying with standards) as well as facilitated "bottom-up" by the C4I acquisitions and technical communities, beginning much earlier in the development process (i.e. pre-Milestone 0). Previous attempts in this area have been plagued by a chronic underestimation of the complexity involved with this type of testing. By focusing on

system evaluation within a Capstone Requirements Documents (CRD) framework, greater involvement by testing activities will be needed earlier in the requirements specification process to be successful.

3. Capstone Requirement Document Integration

While the testing of CRD integration in joint exercises or advanced simulation environments can support the ability of PMs and doctrinal planners to move forward, it cannot overcome the shortfalls of bad requirements or poor architectural design. In today's acquisition lifecycle, the integration phase of a CRD has traditionally followed the development and testing phases of all the individual systems and interfaces that make up the SoS. To move from interoperability into a truly integrated environment, these efforts must begin to occur in parallel. Attempts at integrating a SoS as a prototype for experimentation can provide significant insights into the consequences of operational requirements and design decisions made earlier in the acquisition process.[42] This concurrent strategy will render a clearer understanding early in the acquisition cycle vice near the end, as seen in the more conventional waterfall approach that relies primarily on knowledge of the capabilities of individual systems for early CRD integration decisions.

---

[42] Krygiel, Annette. *Behind the Wizard's Curtain.* DoD C4ISR Cooperative Research Program Publication Series, 1999.

B. THREE ASPECTS OF ARCHITECTURE

1. Universal Interoperability

The promise of a "plug-n-play" Common Operating Environment is a seductive one. As a practical matter, large organizations (such as DoD) are generally unable to start with such a blank slate, so consideration for legacy system inclusion in the DII COE is a requirement and certain compromises will have to be made. While an architecture that enables common data structures/interface provisions and high-level specification/ information exchange requirements would be optimal, this "holy grail" could be just that: an unattainable goal.

The ideal of universal interoperability is neither achievable nor necessary for C4I systems. It should be obvious even to the most casual observer that not every system on the battlefield needs to interoperate with every other one. Nor is universal interoperability technically feasible given the rate of change in both technologies and missions. The determination of what and how much interoperability is sufficient, as well as decision-making about allocation of resources, can only be addressed within the operational context.

As seen earlier, interoperability does not come without a price. The challenge is to define the minimum number of instances where interoperability is imperative, and to estimate the incremental value of interoperability beyond this point. Interoperability between specifically identified systems that need to work together based on the **mission**

is more efficient and achievable than building every conceivable system according to a single high-level architecture.

2. Joint Operational Architecture/Joint Systems Architecture

The future of the interoperability question hinges on the ability of the requirements generation system and acquisition lifecycle to incorporate the systems and operational portions of architecture as successfully as they have the technical aspect. Much effort has gone into the development of the JTA, and the beginnings of a Joint Operational Architecture (JOA) are now being produced. However, the JTA can only enable interoperability, not assure it. The JTA and DII COE only address interoperability problems at the lower layers of the OSI model, and rightly so. Higher layer issues such as data semantics and applications compatibility are within the developing JOA, while issues such as modularity and coupling are the purview of the largely unexamined Joint Systems Architecture (JSA) realm. The importance to be found in this is that it requires all three parts of architecture to truly achieve integration, and an emphasis on any one over the other two will not prove to be effective.[43] While it has been advantageous to advance the technical aspect (via the JTA) to facilitate the development of the remaining two, we cannot assume that only the technical will solve the full spectrum of interoperability problems.

---

[43] National Research Council. *Realizing the Potential of C4I: Fundamental Challenges.* National Academy of Sciences, 1999.

C. AN INTEGRATION PROCESS ARCHITECTURE

1. Introduction

We have shown that PMs and operational planners both have tools at their disposal to aid in achieving interoperable C4I systems and architectures. At this time these tools remain incoherent and incomplete but do show potential for improvement. As these tools mature they will enhance DoD C4I interoperability and integration. In the meantime what is lacking is a coordinated high-level plan of attack on where and how these tools fit in the development cycle.

As an example, even though the systems are developed by the same contractor, MSTAR and JCAPS show little consideration for integrating with one another. MSTAR is still very much a stovepipe system, while JCAPS (which has the endorsement of OSD) lacks grassroots support amongst the Services. The LISI Inspector is theoretically promising but its implementation is woefully short of DoD and service specific C4I system data. LISI also has the disadvantage of being a complex and thus easily misunderstood model. As an interoperability tool JMTIRA is embryonic in its development and few people outside SPAWAR Systems Center Charleston are even aware of it.

Of the four tools discussed, only LISI will be integrated with any of the other tools, and only JCAPS has a well-defined development strategy. Each tool has its own unique strengths; however, it is integrated together that these tools hold the most promise.

D. REQUIREMENTS-TO-CAPABILITIES (R–TO-C) MODEL

1. Introduction

It would be rather hypocritical for the forces of interoperability to suggest that C4I systems need to be developed jointly when the interoperability assessment tools themselves are evolving in the same old-fashioned stovepipe manner. What is needed is an overarching model of where these tools fit in the C4I development process, and then determine how they can be used synergistically.

In Chapter II we introduced the C4I development cycle as envisioned by CIPO San Diego. This model, conceived by Captain Dave Rosen USAF, exposes the foundation for successfully integrating interoperability into the acquisition life cycle and requirements definition process.

2. CIPO Acquisition Process

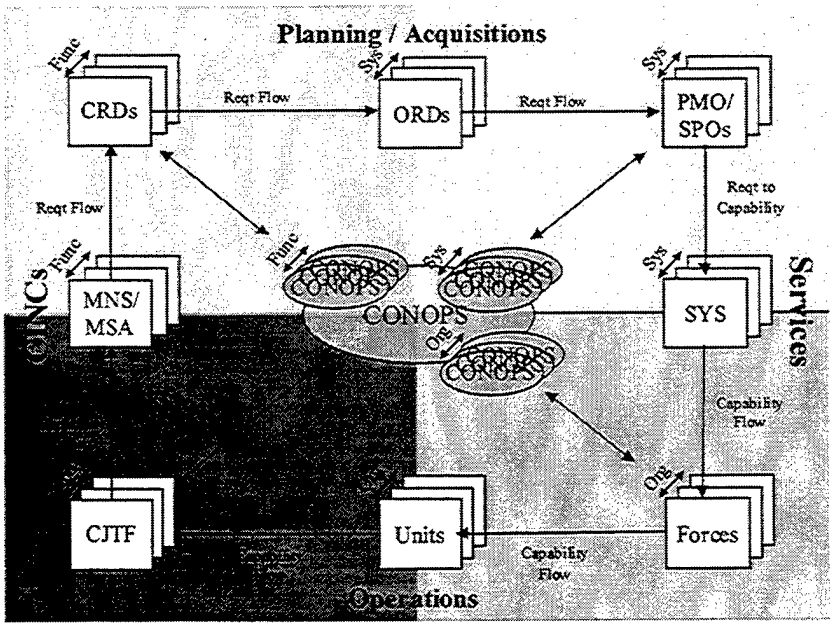

Figure 6-1, CIPO R-to-C Acquisition Process

The cyclic process of translating requirements into capabilities (R-to-C) involves several different players, drawn together by the concept of operations, or ConOps. As depicted above, the overarching ConOps is composed of many localized, subordinate ConOps. Some ConOps are functionally oriented while others are systems or organizational. The relationships between the various ConOps are often quite complex. They must be consistent with one another and the intersections between them be in alignment to adequately define these relationships. The Rosen/CIPO R-to-C Model describes how the ConOps are related to each of the four functional quadrants of their model.

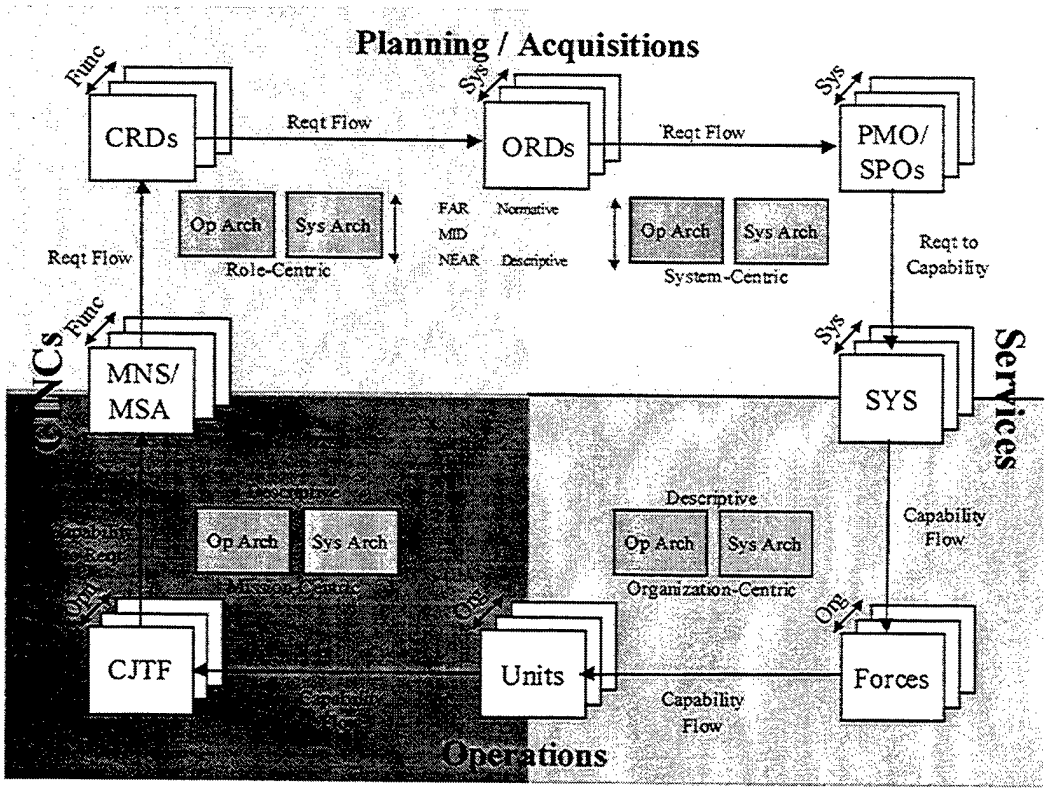

Figure 6-2, Quadrant Centric Architectures

a) Role-Centric

The CIPO model defines the Role-Centric (upper-left) portion of the quadrant architecture as the notional "starting point" of the cycle. This construct is useful because of its ability to associate roles (requirements) with systems (capabilities). Mission areas/roles are initially defined in operational architectures. In examining the CIPO model we have identified inherent problems in the Role–Centric process. The first part of these problems revolves around the exclusionary nature of individual service-based roles creating competition and division. What is needed is an easily referenced demarcation and documentation of each service's role and the interrelations between them.

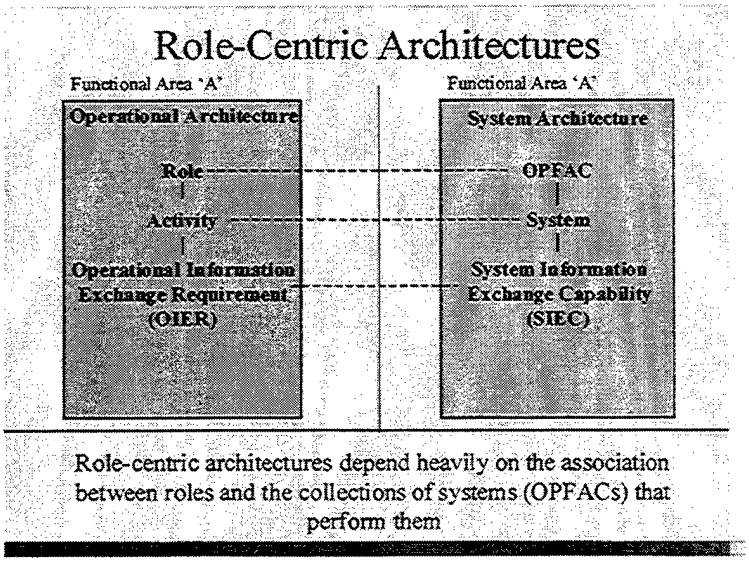

Figure 6-3, Role-Centric Architecture Mapping

The other part of the problem is that systems often must be designed to perform many different roles. Systems are almost always Service-Centric, further

intensifying the competition already instigated by doctrinal role rivalries. In this competitive environment "role-creep" is ever-present due to the pressure to secure budgetary priority that forces services to make systems "multi-mission" (while remaining primarily "single-service"), further tightening the spiral by introducing "requirements-creep" as well. In most instances this situation is the result of ignorance of the larger forces at work within the CIPO cycle.

b) System-Centric

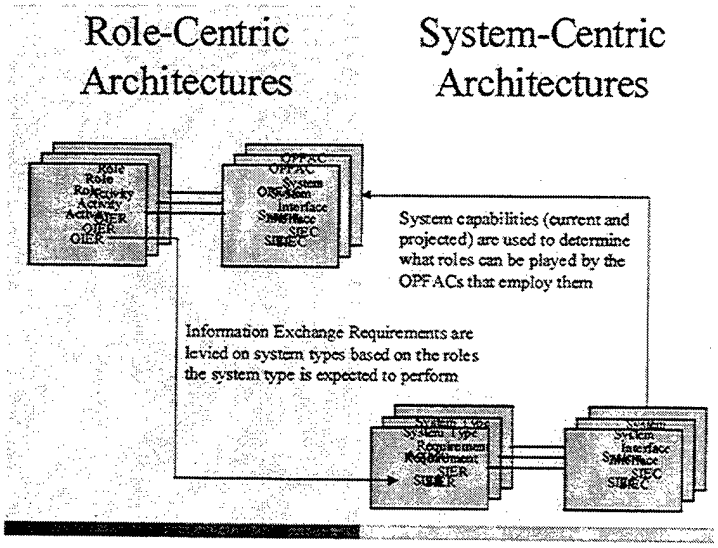

Figure 6-4, Role vs. System Centric Architectures

The CIPO also defines the System-Centric (upper-right) architecture. The System-Centric architecture maps the system requirement to the system capability. There are problems that surface in this part of the CIPO cycle as well. As seen previously, systems are Service-Centric, while requirements ideally belong to the CINCs. This conceivably can create conflicts in the requirements-to-system mapping process. The

CIPO model implies that system capabilities be kept up-to-date so that planners creating Role-Centric architectures are using the best information available to assign system capabilities to role requirements. In reality it is the roles that seem to be shaped by the systems. Why some argue that this is the "tail wagging the dog", that requirements must be designed first, we must recognize that DoD is becoming a buyer, rather than a developer. If we are to give our soldiers, sailors, airmen and Mariness the "overmatch" capbability required to dominate the information battlespace, then in many instances, technology will and should drive requirements. For the acquisition cops that dipute the legality of this concept, we cam make this "overmatch capability" a capstone requirement.

c) Organization-Centric

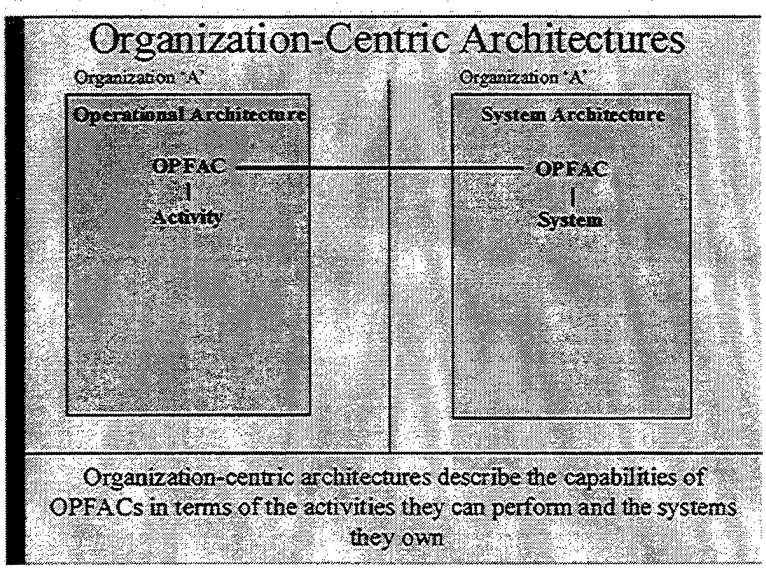

Figure 6-5, Organization Centric Architectures

In the Organization-Centric (lower-right) architecture OPFAC activities are mapped to OPFAC systems. OPFACs are usually associated with an operational organization, the same organizations that the CINC will draw from during Task Force formation. OPFACs exhibit a many-to-many relationship with systems. For example, a communications battalion may receive ATM switches from its systems command, or they may receive a mixture of ATM, IP, and circuit switches. To compound the difficulty of this type of many-to-many relationship, the communications battalion may use discretionary funds to purchase what they deem to be mission-critical systems not approved by its systems command. The problem this creates is many systems designed to perform the same or fewer functions, increasing the likelihood of interoperability problems. The goal in the Organization-Centric quadrant can be summarized by the following equation:

Interoperability = # of Systems / # of Roles
(where Interoperability is <= 1)

To achieve a value less than 1 we are looking for one SoS such as an IP network like the Internet. When an OPFAC does adhere to the fielding plan, it may end up receiving a system capability that it does not have an assigned role for. This can happen during the fielding of new systems that were improperly identified or for units not correctly identified in the activity-to-role process. As we have demonstrated, this can be one of the most critical transitions in the R-to-C process.

d) Mission-Centric

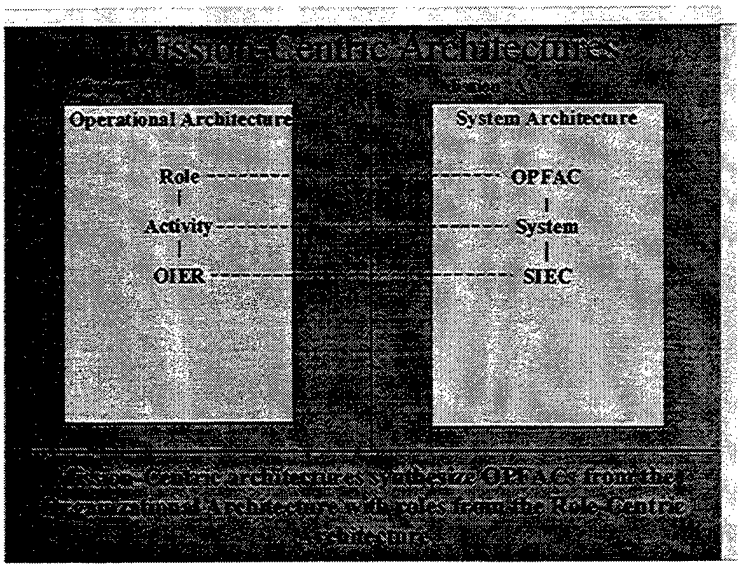

Figure 6-6, Mission-Centric Architectures

The final architecture that the CIPO considers is the Mission-Centric architecture. Mission-Centric architecture takes specific OPFACs from the organizational architecture and maps them to requirements from the Role-Centric architecture. Here CINCs attempt to integrate the products of the other; in other words they will map the organizational (Components/Services/Agencies) to the operational (Joint Task Forces). There are several common problems at this point in the cycle of constructing Mission-Centric architectures. If organizational OPFACs have systems that are not functioning within their roles or the CINC has the wrong OPFACs assigned he will not be able to match available capabilities to needed requirements in order to accomplish the mission. Nor will the CINC have the ability to rapidly configure ad-hoc Mission-Centric architectures and/or explore contingency scenarios in order to develop

alternative courses of action. During our examination of the R-to-C cycle we have determined that an adequate automated tool does not currently exist that has such functionality.

3. Interoperability and PPBS

a) Mapping PPBS to the CIPO Model

The CIPO has constructed a very good model for mapping the R-to-C process. By examining this cycle this we can begin to identify the systemic locations where interoperability problems typically surface. However, what this model currently lacks is a methodology to relate it onto an even more encompassing cycle, the Planning, Programming and Budgeting System. In formulating solutions to the interoperability question we must accept the PPBS as it currently is, at least in the short-term. Since we cannot implement wholesale changes into the PPBS process we must find a way to effectively achieve our goals within its current structure while continuing to examine, and forward, intelligent long-term changes. What we must do is inject interoperability into the PPBS stream by mapping the CIPO model onto the PPBS cycle.

b) DPG and ConOps

A proposal for accomplishing this would begin by replacing the CIPO Model's ConOps with PPBS's Defense Planning Guidance (DPG). The DPG could, like the ConOps, become the document that connects the tasks that each quadrant must perform to turn National Security Strategy (NSS) into a Budget Execution (BE). This process powers the R-to-C process as surely as MNSs and ORDs. To continue to pursue

our goals, interoperability efforts must also be in consonance with the PPBS. In Figure 6-7 PPBS-specific functions are depicted in red and the Joint Strategic Planning System (JSPS) process in teal.

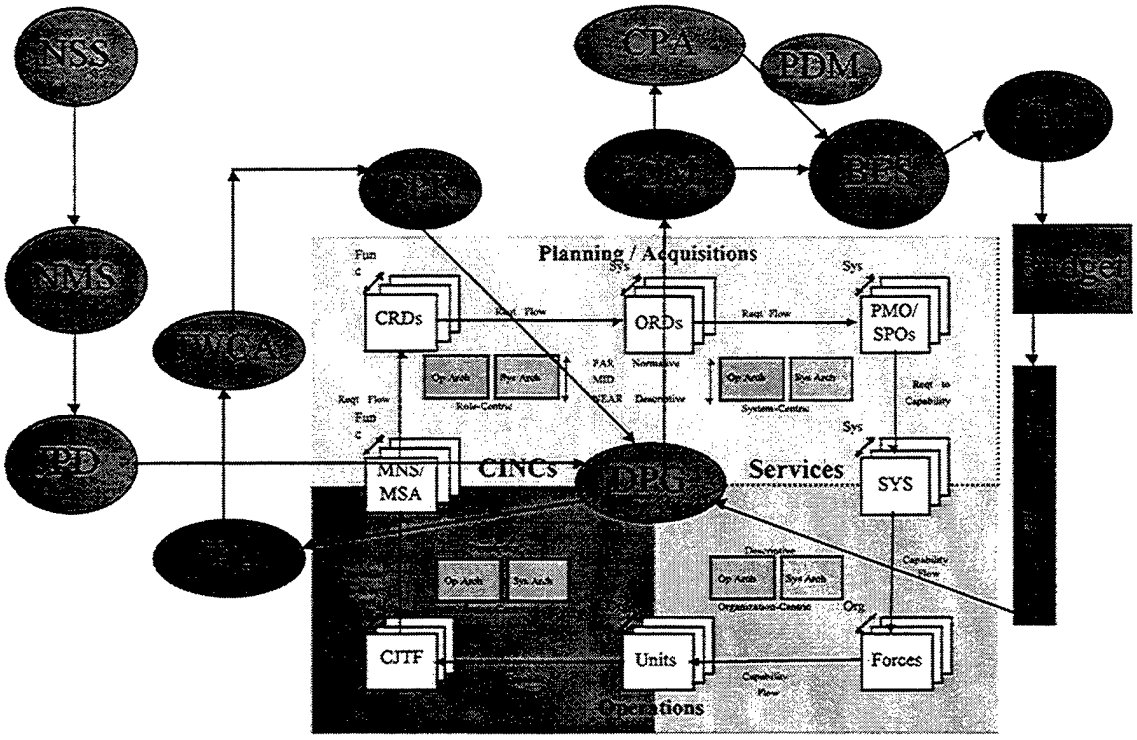

Figure 6-7, PPBS/JSPS in the CIPO Model

c) Power of the Purse

How well the budget is executed within the DPG determines what the next year's Integrated Products Lists (IPLs) will look like. For example, if a CINC asked for

an OPFAC to fill a role and no current OPFAC had the system to fill that requirement the CINC may list it in the IPL depending on the criticality of that system. This brings us back to our previous discussion where the SYSCOMs are fielding new systems to the OPFACs. If an OPFAC gets the wrong system you can see how it affects the CINCs in the Mission-Centric quadrant architecture.

The Joint Warfighting Capabilities Assessment determines what future Role-Centric capabilities the CINC based on the IPL needs. The Chairman's Program Recommendations (CPR) are largely formed by the JWCA. The CPR is then fed back into the DPG to ensure that CINC requirements are commensurate with the National Military Strategy (NMS). This is the first instance of the intersection of the DPG and ConOps functions. The DPG is then revised to become the basis for the Program Objective Memorandum (POM). POM is the link between Role-Centric and System-Centric architectures.

This relationship is important to interoperability. It is at this point where priorities of the CINCs first come into conflict with those of the services. Both the Role-Centric and System-Centric interactions serve to influence the POM. Role-Centric considerations typically manifest as decisions made in regard to CRD formulation and development. CRDs do not currently act as input to the POM; but ORDs do, and this is what the Role-Centric C/S/As must rightly focus upon as they transition to the Service-Centric quadrant for funding and development. As this process progresses the environment is exacerbated by the exclusive Service-Centric Systems Commands and

Program Executive Offices. At this point in the cycle the Chairman's Program Assessment (CPA) can somewhat act as an advocate for Mission-Centric considerations, affecting the DPG through the POM. Once the BE is sent to the President the process again comes under Service-Centric influence via the "power of the purse".

E. TOOL FOR THE CIPO MODEL

1. PPBS and Interoperability

The PPBS system was not designed to facilitate interoperability; to the contrary, it often directly obstructs interoperability initiatives, but knowing where the system breaks down is the first step in fixing it. So how do we move the Mission-Centric quadrant beyond Service-Centric quadrant parochialism?

The CIPO model addresses the "where" and "how" of interoperability fitting in the R-to-C cycle and how it could work with the PPBS/JSPS systems. What all players in each quadrant need are automated tools to help them function effectively in their own quadrant and interact productively with adjacent quadrants. The Rosen/CIPO Model has suggested where some of these tools may fit.

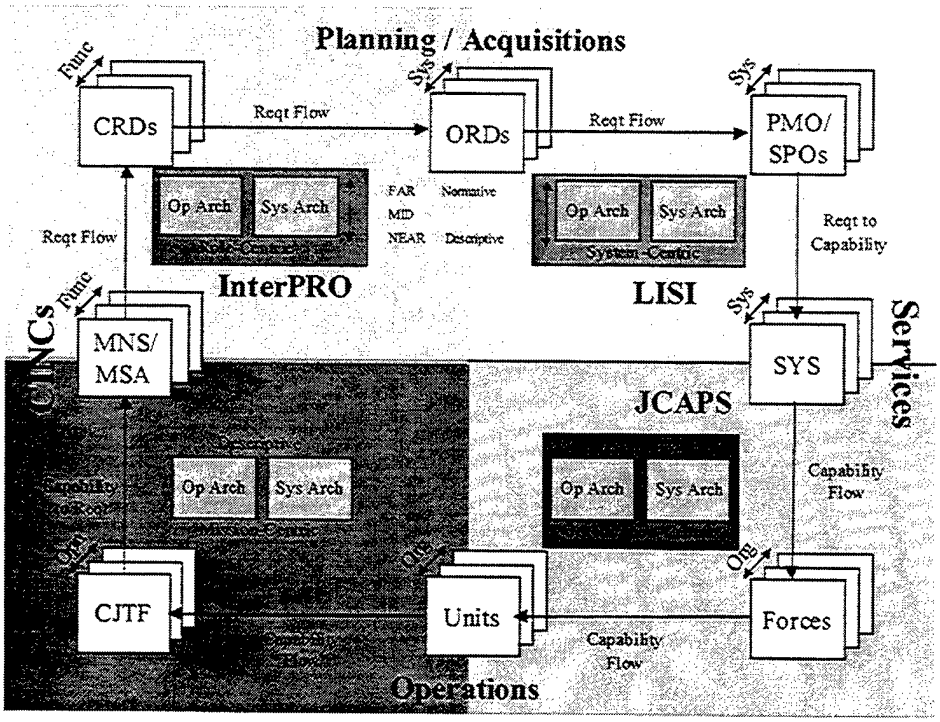

Figure 6-8, Tools in the CIPO Model

2. Automated Tool Integration

The CIPO has suggested that several of the currently available architecture and interoperability tools fit into their model as depicted in Figure 6-8. Both their analysis and ours both conclude that while the tools in their existing states do not satisfy all the requirements for these activities, this is the position in the methodology that their proposed functionality will support. In the CIPO model the conclusion is that there does not yet exist an adequate tool to address the Mission-Centric quadrant. JCAPS was noted as possibly being able to fill this role except for the fact it does not possess the capability to integrate Role-Centric with Organization-Centric architectures. In its current state we agree with this. We examined two additional tools, MSTAR and JMTIRA, that we

believe could help fill this gap. Figure 6-9 is our depiction of the proposed integration of the tools discussed within the CIPO model.

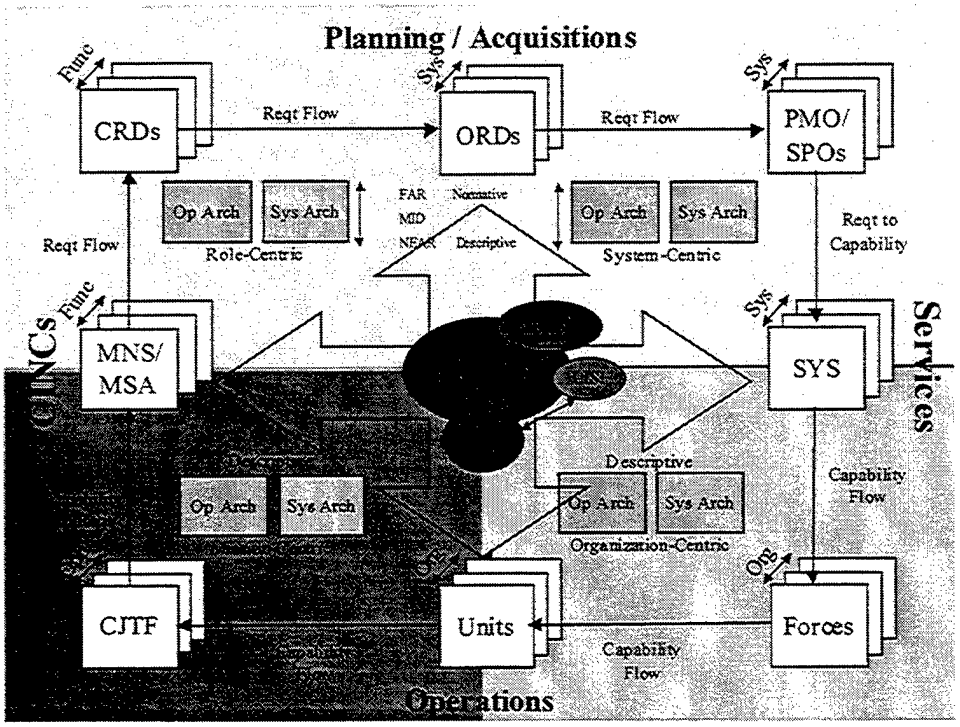

Figure 6-9, Tool Integration Into the CIPO Model

In this depiction JCAPS is the tool that will aid the players in tying all four quadrants into a collaborative working group, providing the required linkage to both the ConOps in the R-to-C cycle and to the DPG in the PPBS. JCAPS is fully supported by the OSD and Joint levels and thus is better funded than the other programs, giving it the greatest potential for maturation and operational acceptance. While JCAPS currently has well defined limitations, as these are being identified and incorporated into changes to the system and the process we feel that the potential to achieve this perceived functionality is attainable.

3. JCAPS Synthesis and Integration

a) MSTAR into JCAPS

The CIPO has stated that JCAPS cannot construct the Mission-Centric architectures, i.e. mapping operational architectures to system architectures.[44] JCAPS can provide both operational and technical views but what it lacks is the root system granularity that exists in MSTAR. This is reason we could not effectively construct a MAGTF Integrated Package (MIP) using JCAPS. MSTAR has the requisite granularity, primarily because it was designed as a Service-Centric architecture tool. If each Service develops its own MSTAR –type application these repositories can be integrated as part of a common JCAPS database, giving JCAPS the necessary granularity to construct Mission-Centric architectures. Combined with the JCAPS client drawing capabilities, this would enable CINCs to construct the identified requirement of ad-hoc task force architecture development.

MSTAR is also more advanced than JCAPS in mapping programmatic issues to the individual system. If JCAPS were to incorporate this feature by gaining access to Service-Centric acquisition data this would functionally allow the "left-hand" quadrant to know what the "right-hand" quadrant is doing. While the services will most certainly be resistant to such a "looking glass" into their affairs, this is a necessary prerequisite to achieving interoperability.

---

[44] Rosen, David, Capt, JFPO. "Defining the Interoperability Battlespace". Presentation.

b) LISI Inspector into JCAPS

The JCAPS program will allow interface to the LISI Inspector tool via SIPRNET/NIPRNET access. This actually falls short of what MSTAR does by embedding LISI Inspector into the program, allowing LISI Inspector to take advantage of MSTAR's system technical data and vice-versa. If JCAPS chooses to incorporate a similar implementation this will improve the ad-hoc architecture construction requirement mentioned previously. The marriage of LISI with JCAPS, thus incorporating Service-Centric system data into the JCAPS repository, will enable LISI to become the tool its developers originally envisioned, and also giving JCAPS a powerful interoperability assessment feature for all four quadrants of the CIPO model.

c) JMTIRA into JCAPS

With further development, JMTIRA could provide the "missing link" for the left-hand quadrant of the CIPO model. While LISI tells planners where interoperability problems exist JMTIRA could have the ability to tell whether these problems have been tested, recommend effective test scenarios, and most importantly assign a quantitative risk level if the interoperability issue is not resolved. In an era when CINCs confront dwindling financial resources, this type of operational risk management gives them a true decision aid in determining whether they can afford to ignore the issue or expend the resources required to resolve it. Role and System -Centric architects can also save significant dollars by identifying risk factors early on in a program's development cycle by utilizing JMTIRA.

4. JCAPS in Action

This sort of integrated JCAPS tool could be used in the CIPO model to effectively interact the PPBS and JSPS cycles. All the C4ISR Architecture Framework views could be shared among all quadrant players of the CIPO model. Differences and issues that surface could be resolved in a more collaborative environment. Programmatic issues such as configuration management, budgetary considerations, and acquisition objectives would be available to CINCs as well as PMs. JCAPS could also be used to collaboratively "what-if" scenarios in the PM's environment as well as the CINC's. Technical descriptions and system capabilities could be made available to budget planners, quantifying and highlighting risk if these systems are not funded. JCAPS could become the central workplace for all CIPO Model stakeholders to share ideas and information, thereby constructing a truly joint, interoperable system of systems.

a) SDDA Chain

To demonstrate what an integrated JCAPS tool would do we need to look at the Sense-Decide-Decide-Act Chain (SDDA). Figure 6-10 depicts this cycle as it is today.[45] The sensor suite is a homogenous set of sensors representing a service-centric or program-specific system. Today, we can exchange information between the sensors and the decision maker that the service-centric system was targeted for. However, add a different decision node that was not the target of the initial system, and in most cases, information cannot be exchanged. This is our current interoperability dilemma.

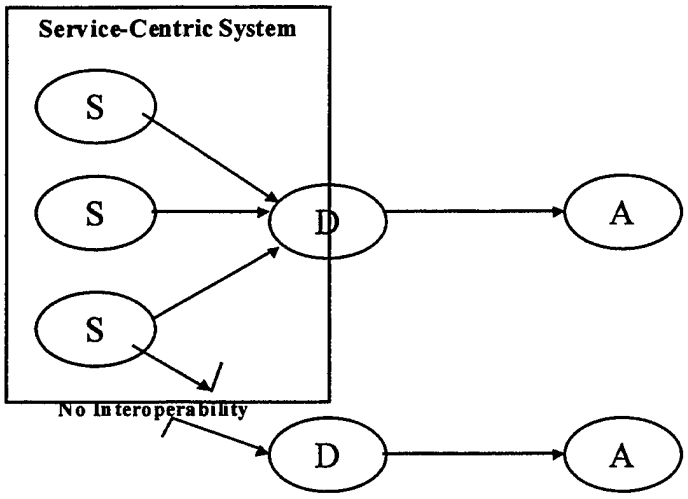

Figure 6-10, SDDA Chain

What we need to do is integrate the homogenous or service centric sensors with other sensors using a heterogeneous-sensor fusion process. Instead of exchanging information with one decision node we can now exchange information with multiple decision nodes. Figure 6-11 models how this would be done.

We combine the decision and action nodes into an OODA loop node based on the Boyd Cycle (observation, orientation, decision, and action). The ability of any OODA node to take advantage of all sensor platforms is the goal of interoperability. An integrated JCAPS tool, in a collaborative environment of all four quadrants of the CIPO model can achieve this goal. JCAPS can tell us the what and why of the sensor fusion, MSTAR/LISI can tell us how, and JMTIRA can tell us the consequence of one or more sensor platforms being lost, or unable to exchange information.

---

[45] Buddenberg, Rex. *IT Arch Musing*. E-Mail, 22 June 2000.

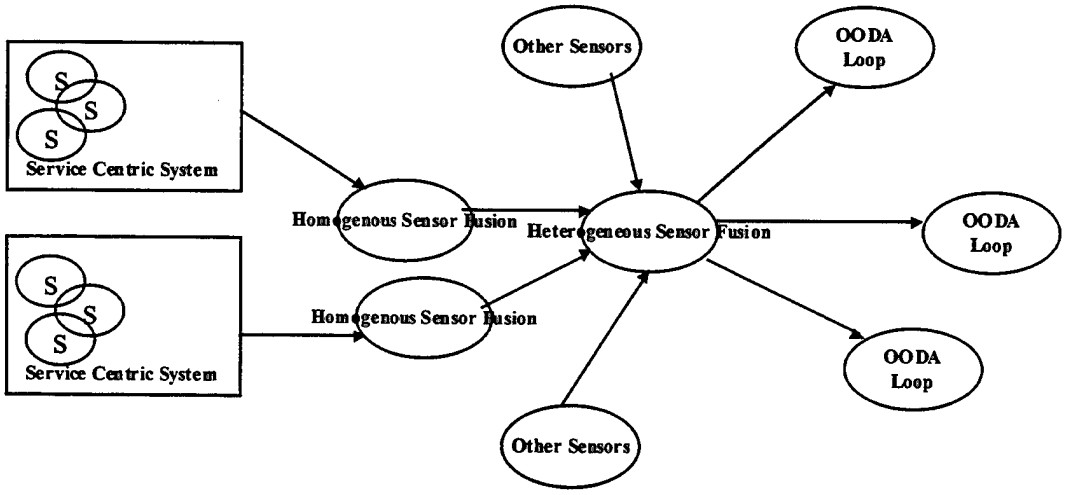

Figure 6-11, Sensor Fusion

We can call each of these heterogenous fusion models a module, and there may be several of these modules within a CINC area of operations. We now link these modules as nodes in a network with the OODA nodes as subscribers. If one module node is lost , the remain OODA nodes can still exchange information with any of the other module nodes.

Mapping this process to the development quadrants, the modules can be fielded as a more modularized MIP. This revised MIP (RMIP) should be a complete transition from the taxonomic (descriptive) to the operational (prescriptive). CINCs can now plug in these RMIPs like nodes in a network. The RMIPs can be built around functions or as OPFACs. The nodes can exchange information with other OODA nodes using a common protocol such as IP. We now could have a IP-based network that truly could facilitate technical implementations of interoperability.

Obstacles to this vision will abound. It will be difficult to get inside the PM "rice-bowl" to share programmatic data. The data repositories themselves will rely on quadrant players maintaining the currency and quality of their information. Finally, there must be an overarching advocate for the entire system, maintaining information, enforcing data integrity, and acting as a mediator when roles, budgets and missions inevitably come into conflict. An integrated JCAPS tool must remain a joint program; mutually funded and developed by the Services to provide the collaborative environment they all need to meet the requirements of JV2020.

F. CHALLENGE OF THE JOINT STRUCTURE

Though the goal of C4I systems is that they be interoperable in a joint environment, this horizontal objective must be realized in a world that is fundamentally vertical. As discussed, the vertical focus of acquisition comes from the fact that systems are acquired and funded by the individual C/S/As, and the acquisition system itself is geared toward the development of discrete components rather than system-wide capabilities. PMs are generally held accountable for their piece of a system, not for the performance of the whole system of systems. This remains one of the fundamental stumbling blocks for the procedural initiatives that have been proposed to enhance interoperability. An obvious recommendation would be to realign how "success" is determined for individual programs by de-emphasizing the traditional measures of performance, cost, and schedule. This type of change is difficult to quantify and most

certainly would be a long-term implementation since it involves organizational and cultural -level issues.

The challenge of managing interoperability is one of addressing its state throughout the entire enterprise rather than attempting to measure every variable in each possible scenario. It is generally accepted that management must be able to measure what they wish to change. The ways in which interoperability can be measured and reported differs intrinsically from the factors included in other areas of combat readiness. C/S/As are not necessarily in a position to ascertain the status of external C4I systems. This is a key issue in determining the ability to conduct successful joint combat operations. Interoperability is an indirect contributor to combat power, and hence difficult to quantify. Interoperability must be assessed at the joint level for it to have any meaning for the enterprise, and the joint structure must be empowered to enforce its initiatives, initiatives that will often be at odds with the priorities of the C/S/As. Until this dichotomy has been resolved, interoperability will not reach its full potential.

APPENDIX A

LISI GENERIC INTEROPERABILITY PROFILE EXAMPLE

Generic Interoperability Profile
COE-NT 4.1

HOME | SEARCH | REPORTS | HELP

Unclassified

The Generic Level for COE-NT is: **3b**

LISI	*Procedures*	*Applications*	*Infrastructure*	*Data*
Enterprise				
		⊡ [Cut&Paste] Object		
Domain		⊡ [DBApps] Informix ⊡ [DBApps] Sybase ⊡ [DBApps] Oracle	⊡ [WAN] NIPRNET ⊡ [WAN] SIPRNET ⊡ [WAN] GCCS-T ⊡ [WAN] JWICS	
	⊡ [SecStd] Operating System Services ⊡ [SecStd] Evaluation CriteriaTCSEC	⊡ [Collab] VIC ⊡ [Collab] Netscape Conference ⊡ [Collab] Collaboration-Other ⊡ [Collab] VAT ⊡ [DoDCaps] MIDB ⊡ [DoDCaps] JOPES ⊡ [DoDCaps] Other ⊡ [DoDCaps] COP ⊡ [DoDCaps] COMPASS ⊡ [DoDCaps] COMPASS-I	⊡ [Proto-TCP/IP] UDP	⊡ [DBModel] DoD C2 Corps (GCCS) ⊡ [DBModel] DoD Intel ⊡ [DoDCaps] COMPASS ⊡ [DoDCaps] COMPASS-I ⊡ [MsgTypes] COMPASS ⊡ [MsgTypes] COMPASS-I

			☐ [DoDCaps] JDISS ☐ [DoDCaps] UHF-NRP ☐ [DoDCaps] TPN ☐ [DoDCaps] GCCS ☐ [DoDCaps] GCCS-M ☐ [MsgTypes] COMPASS ☐ [MsgTypes] COMPASS-I		
		☐ [SecStd] HCI Authentication ☐ [SecStd] Security Auditing-Alarms ☐ [SecStd] Screen Classification ☐ [SecStd] Access Controls	☐ [Cut&Paste] Text ☐ [DBFmt] DCE ☐ [DBSrvcs] DCE ☐ [DBSrvcs] JDBC ☐ [DBSrvcs] ODBC	☐ [Proto-TCP/IP] TCP/IP ☐ [Proto-TCP/IP] TCP	
			☐ [Browser] Netscape		☐ [DocFmt] HTML-I/O ☐ [WebFmt] HTML-I/O ☐ [WebFmt] JavaApplets-I/O
		☐ [OEType] DII COE	☐ [DBApps] Access ☐ [GraphFmt] CorelDraw-I ☐ [GraphSvcs] CorelDraw-I ☐ [GraphSvcs] PowerPoint ☐ [GraphSvcs] Acrobat ☐ [GraphSvcs] MPEG ☐ [GraphSvcs] Microsoft Paint	☐ [LAN Type] Fiber-FDDI ☐ [LAN Type] Ethernet	☐ [AVFmt] MPEG-1-I/O ☐ [AVFmt] AU-I ☐ [AVFmt] MOV-I ☐ [AVFmt] WAV-I ☐ [DocFmt] XGML-I/O ☐ [GraphFmt] .BMP-I/O ☐ [GraphFmt] .WMF-I/O ☐ [GraphFmt] .PPT-I/O

Connected		☐ [SecClass] Unclassified Code ☐ [SecClass] Unclassified Data ☐ [SecClass] Secret Code ☐ [SecClass] Secret Data ☐ [SecClass] Sensitive / Restricted Code ☐ [SecClass] Sensitive / Restricted Data ☐ [SecClass] Confidential Code ☐ [SecClass] Confidential Data ☐ [SecClass] US-SI/TK ☐ [SecClass] US-SI/TK ☐ [SecClassS] US Secret-Code ☐ [SecClassS] US Secret-Data ☐ [SecStd] AR 380-19	☐ [Chat] Other		☐ [ImageryFmt] CGM/JPEG-I
			☐ [Proto-TCP/IP] TELNET ☐ [Proto-TCP/IP] TELNET ☐ [RmtAccess] TELNET ☐ [RmtAccess] TELNET	☐ [Comms] Land Line ☐ [Comms] SATCOM ☐ [Interfaces] Fiber ☐ [Landline] Long Haul ☐ [Landline] Microwave ☐ [Landline] Coax Cable ☐ [Landline] Fiber	☐ [FileCompres] CZIP-I/O

Functional			☐ [ImageSvcs] GCCS Imagery ☐ [Mapping] MPEG ☐ [Mapping] JMTK ☐ [Spreadsheet] MSExcel ☐ [WordProc] MSWord ☐ [WordProc] Acrobat		☐ [GraphFmt] .GIF-I/O ☐ [GraphFmt] .JPG-I/O ☐ [ImageryFmt] NITF 1-I ☐ [ImageryFmt] NITF 2-I ☐ [SpreadsheetFmt] Excel (.XLS)-I/O ☐ [WebFmt] XGML-I/O
			☐ [EmailSvcs] MS Mail ☐ [EmailSvcs] Netscape ☐ [MsgTypes] USMTF-I/O ☐ [MsgTypes] OTH-GOLD-I ☐ [MsgTypes] TextMsg-I/O	☐ [Protocols] Mil Types ☐ [Protocols] TCP/IP DL Types ☐ [Protocols] PPP DL Types	☐ [DBdesktop] MDB-I/O ☐ [MapFmt] WVST-I ☐ [MapFmt] DNC-I ☐ [MapFmt] VPF-I ☐ [MapFmt] DTED-I
		☐ [Stds] JTA-w/Waiver	☐ [EmailSvcs] POP3 ☐ [MsgProc] CMP ☐ [Proto-TCP/IP] POP3 ☐ [WordProc] Simple Text (ASCII) ☐ [WordProc] NetScape	☐ [FileTrans] FTP ☐ [FileTrans] FTP ☐ [LAN Type] MAC(802.3) ☐ [Proto-TCP/IP] FTP ☐ [Proto-TCP/IP] FTP	☐ [MsgTypes] USMTF-I/O ☐ [MsgTypes] OTH-GOLD-I ☐ [MsgTypes] TextMsg-I/O
		☐ [SecStd] Key-Management-X.509 ☐ [SecStd] Other ☐ [SecStd] Application Software Entity	☐ [Messaging] MsgViewer	☐ [Proto-TCP/IP] HTTP	

Isolated				☐ [Media] CD-ROM ☐ [Media] 8mm Tape ☐ [Media] 4mmDAT ☐ [Media] DVD-RAM ☐ [Media] 3.5in Disk	☐ [FileSys] FAT 16-I/O ☐ [FileSys] CDFS-I/O ☐ [FileSys] NTFS-I/O
				☐ [Manual] Keyboard Input	
				☐ [Manual] Printer Output	

Overlays: Core Data Set

The Detailed Generic Metric for COE-NT is: **G3b P3c A4a I3c D3b**

APPENDIX B

LISI netViz OUTPUT EXAMPLE

LISI netViz Output

Nodes

System Name	Generic Level
AFATDS	G1c
AN/MRC-145	G0o
AN/PRC-119A,B,C&E	G0o
AN/PRC-68A	G0o
DACT N/A	G4a
GCCS	G3c
IAS MSBL 1.1	G3c
PLRS COMM (PCE) UNKNOWN	G0o
TCO	G3b

Links

From Node	To Node	Generic Level Between Nodes	Specific Level Between Nodes
AFATDS	AN/MRC-145	G0o	S0o
AFATDS	AN/PRC-119A,B,C&E	G0o	S0o
AFATDS	DACT N/A	G1c	S3b
AFATDS	GCCS	G1c	S3b
AFATDS	IAS MSBL 1.1	G1c	S3b
AFATDS	TCO	G1c	S3b
AN/MRC-145	AN/PRC-119A,B,C&E	G0o	S0o
AN/MRC-145	DACT N/A	G0o	S0o
AN/MRC-145	TCO	G0o	S0o

AN/PRC-119A,B,C&E	DACT N/A	G0o	S0o
AN/PRC-119A,B,C&E	TCO	G0o	S0o
DACT N/A	GCCS	G3c	S3c
DACT N/A	IAS MSBL 1.1	G3c	S3c
DACT N/A	PLRS COMM (PCE) UNKNOWN	G0o	S0o
DACT N/A	TCO	G3b	S3b
GCCS	TCO	G3b	S3b
IAS MSBL 1.1	TCO	G3b	S3b
PLRS COMM (PCE) UNKNOWN	TCO	G0o	S0o

To view this report:

1. Please click **LISI_17-Aug-00_14_13.csv** and save to your local machine. Make sure the extension is .csv
2. Open netViz and create a new project based on the LISI.CAT catalog file.
3. From the "Tools" menu, select Import/From Text. Select the file downloaded in step 1. From "Import Options," for existing objects" and "Create object for each unique data record (unless object exists)."

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. United States General Accounting Office. "Interoperability: DoD's Efforts to Achieve Interoperability Among C3 Systems". GAO/NSIAD-87-124.

2. United States General Accounting Office. "DoD's Renewed Actions To Improve C4I Interoperability May Not Be Adequate". GAO/NSIAD-94-47.

3. United States General Accounting Office. "Weaknesses in DoD's Process for Certifying C4I Systems' Interoperability". GAO/NSIAD-98-73.

4. Buchanan III, H. Lee, ASN(RD&A). Speech. 18 Jul 00.

5. CJCS Publication. "Joint Vision 2020". http://www.dtic.mil/jv2020/

6. Nutwell, Robert, RADM, DASD(C3ISR&S). "New Interoperability Policies and Processes". Presentation.

7. Gansler, J., USD(AT&L). "Promulgation of DoD TRM Version 1.0". DoD Memorandum dtd 21 Mar 00.

8. Rosen, David, Capt, JFPO. "Defining the Interoperability Battlespace" Presentation.

9. Kaminski, Paul, USD(A&T). "Implementation of the DoD Joint Technical Architecture". DoD Memorandum dtd 22 Aug 96. http://coeeng.ncr.disa.mil/REFERENCE_PAGES/LEV.HTM

10. Center for Computer Systems Engineering Information Clearinghouse. Shared Data Environment – SHADE. http://dii-sw.ncr.disa.mil/shade/

11. C4ISR Architecture Working Group Final Report. http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/pdf/fnlrprt.pdf

12. Manley, James. "Analysis Results of JCAPS Live Fire Test" Conducted by Joint Forces Program Office". MITRE Corporation. December, 1999.

13. DoD Architecture Framework Working Group. "DoD Architecture Framework Version 2.1, Volume I: Definitions and Guidelines". 26 Jul 00.

14. Dean, Keith, OASD(C3I). "C4I Support Plans (C4ISP) Overview Brief". Presentation. http://www.dsc.osd.mil/dsc/plans/C4ISP_webpg/thebrief.pdf

15. Wallace, Clint, COL. "Preliminary Assessment of Adequacy of Infrastructure Resources to Support Test and Evaluation of Interoperability". Presentation.

16. JITC Certification Process. http://jitc.fhu.disa.mil/testing/interop/interop.htm

17. CJCS Instruction 6212.01B. "Interoperability and Supportability of National Security Systems, and Information Technology Systems". 08 May 00.

18. JIEO/JITC Circular 9002. "Requirements Assessment and Interoperability Certification of C4I and AIS Equipment and Systems". 23 Jan 95.

19. Zavin, Jack, OSD. "Achieving Joint and Combined Interoperability: A Strategic Process". Presentation.

20. Forsberg, Kevin, Mooz, Hal, & Cotterman, Howard. *Visualizing Project Management*. John Wiley & Sons, Inc. 1996.

21. JCAPS Homepage, https://extranet.if.afrl.mil/jcaps_extra/

22. JCAPS Users Manual, Prototype Version 2.1, 1 August, 2000.

23. USMC Digitization-C4ISR Near Term Architecture and Efforts Briefing, C4ISR Directorate.

24. Levels of Information System Interoperability Report, C4ISR Architecture Working Group, Department of Defense, 30 March 1998.

25. Joint Maritime Tool for Interoperability Risk Assessment Brief to Naval Postgraduate School by SPAWAR Charleston SC, 25 May 2000.

26. http://jitc.fhu.disa.mil.

27. JCAPS Hands-On Training Guide (Prototype 2.1) 1 Mar 2000.

28. Mitre, Corp. "Analysis of JCAPS Live Fire Results" Joint Forces Program Office, 20 Dec 99.

29. Krygiel, Annette. *Behind the Wizard's Curtain*. DoD C4ISR Cooperative Research Program Publication Series, 1999.

30. National Research Council. *Realizing the Potential of C4I: Fundamental Challenges.* National Academy of Sciences, 1999.

31. Buddenberg, Rex. *IT Arch Musing*. E-Mail, 22 June 2000

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Director, Training and Education 1
   MCCDC, Code C46
   1019 Elliot Road
   Quantico, VA 22134-5027

4. Director, Marine Corps Research Center 2
   MCCDC, Code C40RC
   2040 Broadway Street
   Quantico, VA 22134-5107

5. Marine Corps Representative 1
   Naval Postgraduate School
   Code 037, Bldg. 330, Ingersoll Hall, Room 116
   555 Dyer Road
   Monterey, CA 93943

6. Marine Corps Tactical Systems Support Activity 1
   Technical Advisory Board
   Attn: Librarian
   Box 555171
   Camp Pendleton, CA 92055-5080

7. Rex Buddenberg 1
   Naval Postgraduate School
   Code SM/RB
   Monterey, CA 93943

8. John Osmundson 1
   Naval Postgraduate School
   Code SM/JO
   Monterey, CA 93943

9. Dave Ruiz 1
18365 W. 116 St.
Olathe, KS 66061

10. Rick Williams 1
915 Viking Ln
San Marcos, CA 92069

11. Chair, Information Systems Academic Group.....1
Code IS
Naval Postgraduate School
Monterey, CA 93952