(2)

AD-A233 608

STUDY PROJECT

THE BASIS FOR INTEROPERABILITY

BY

LIEUTENANT COLONEL MARK K. HAYDEN
United States Marine Corps

USAWC CLASS OF 1991

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION U.S. Army War College 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Carlisle Barracks, PA 17013-5050	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)

The Basis for Interoperability

12. PERSONAL AUTHOR(S)

Lieutenant Colonel Mark K. Hayden

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Individual	FROM _____ TO _____	14 March 1991	~~30~~ 32

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

Interoperability among command and control (C2) systems has been a longstanding problem ever since President Kennedy discovered during the Cuban missile crisis that the agencies of the executive department couldn't rapidly and accurately exchange information among themselves. Efforts to achieve true interoperability across the board have been futile. This is especially evident within the Department of Defense (DOD). In fact, information management responsibilities within the DOD are so fragmented, it is difficult to define the problem, let alone solve it. Recently, serious attempts by the Defense community have been successful in pinpointing a root cause of the interoperability problem. Hidden among the many symptoms of this problem was the critical fact that the basis for interoperability rest on the adherence of system components to common standards. The question is, who coordinates, sets, maintains, and enforces the information (data), information processing, and communication (information exchange) standards to meet user requirements?

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☐ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	
22a. NAME OF RESPONSIBLE INDIVIDUAL ROBERT F. HERVEY, COL, SC	22b. TELEPHONE (Include Area Code) (717) 245-4016 / 22c. OFFICE SYMBOL AWCAC

DD Form 1473, JUN 86 *Previous editions are obsolete.* SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Block 19. Abstract (Cont.)

This paper highlights the ongoing efforts to harness control of the root cause of interoperability problems; information standards. It provides an overview of the problem, the findings of recent efforts to pinpoint the systemic bureaucratic barriers to achieving interoperability, and the realization that only a top-down authority can apply the centralized management structure needed to guide user-technical groups when collaborating on information requirements (ends), procedures (ways) and computing/communications processes (means).

USAWC MILITARY STUDIES PROGRAM PAPER

THE BASIS FOR INTEROPERABILITY

An Individual Study Project

by

Lieutenant Colonel Mark K. Hayden
United States Marine Corps

Colonel Robert F. Hervey, USA, SC
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013-5050

ABSTRACT

AUTHOR: Mark K. Hayden, LtCol USMC

TITLE: The Basis for Interoperability

FORMAT: Individual Study Project

DATE: 14 March 1991 PAGES: 30 CLASSIFICATION: Unclassified

Interoperability among command and control (C2) systems has been a longstanding problem ever since President Kennedy discovered during the Cuban missile crisis that the agencies of the executive department couldn't rapidly and accurately exchange information among themselves. Efforts to achieve true interoperability across the board have been futile. This is especially evident within the Department of Defense (DOD). In fact, information management responsibilities within the DOD are so fragmented, it is difficult to define the problem, let alone solve it. Recently, serious attempts by the Defense community have been successful in pinpointing a root cause of the interoperability problem. Hidden among the many symptoms of this problem was the critical fact that the basis for interoperability rests on the adherence of system components to common standards. The question is, who coordinates, sets, maintains, and enforces the information (data), information processing, and communication (information exchange) standards to meet user requirements?

This paper highlights the ongoing efforts to harness control of the root cause of interoperability problems; information standards. It provides an overview of the problem, the findings of recent efforts to pinpoint the systemic bureaucratic barriers to achieving interoperability, and the realization that only a top-down authority can apply the centralized management structure needed to guide user-technical groups when collaborating on information requirements (ends), procedures (ways) and computing/communications processes (means).

Introduction

Interoperability among command and control (C2) systems has been a longstanding problem ever since President Kennedy discovered during the Cuban missile crisis that the agencies of the executive department couldn't rapidly and accurately exchange information among themselves. Efforts to achieve true interoperability across the board have been futile. This is especially evident within the Department of Defense (DOD). In fact, information management responsibilities within the DOD are so fragmented, it is difficult to define the problem, let alone solve it. Recently, serious attempts by the Defense community have been successful in pinpointing a root cause of the interoperability problem. Hidden among the many symptoms of this problem was the critical fact that the basis for interoperability rests on the adherence of system components to common standards. The question is, who coordinates, sets, maintains, and enforces the information (data), information processing, and communication (information exchange) standards to meet user requirements?

This paper highlights the ongoing efforts to harness control of the root cause of interoperability problems; information standards. It will provide an overview of the problem, the findings of recent efforts to pinpoint the systemic bureaucratic barriers to achieving interoperability, and the realization that only a top-down authority can apply the centralized management structure needed to guide user-technical groups when collaborating on information requirements (ends), procedures (ways) and computing/communications processes (means).

The Requirement

Commanders must direct and control their forces on a battlefield of confusion, chaos, and casualties. They need the latest and most accurate information on the status of their own forces, the enemy's disposition and movement, and environmental conditions, such as terrain and weather. They need this information to be able to see, decide, and act to influence the battle. C2 systems support and aid commanders as they endeavor to obtain an accurate battlefield picture and exercise command and control. These systems are a combination of elements that form a complex whole.[1] By official definition, a C2 system is "the facilities, equipment, communications, procedures and personnel essential to the commander for planning, directing, and controlling operations of assigned forces pursuant to the mission assigned."[2] What binds these five elements together into an effective system is information. Each C2 system must be able to collect, process, display, disseminate, and retain information to meet the needs of the commander.[3] Modern technology provides the communications and intelligence services, high speed data (computer) processing, tactical decision aids and displays for C2 systems to accomplish command and control functions. C2 systems are alternatively referred to as "C2I", "C3I", and "C4I" systems within the DOD community. The use of these terms depends on the users preference for identifying communications, computer and intelligence functions as associated with command and control.

The effectiveness of military organizations and their weapons depends upon the architecture or network of C2 systems

supporting those forces.[4] A network of C2 systems allows common information and data to be introduced and shared across functional areas, i.e., fire and maneuver, air operations, intelligence, administrative (personnel), logistics and maritime. This information needs to flow horizontally around the battlefield between combat, combat service, and combat service support units and their weapon systems. It also flows vertically between command echelons. This can only occur if the C2 systems are interoperable.

Interoperability is vital to C2 systems used by US and allied forces in joint and combined operations. It is "the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together."[5] This ability to exchange critical information both horizontally and vertically in and out of theater, allows an operational commander to quickly organize, task and synchronize his combat forces to attack the enemy at his most vulnerable points. Hence, interoperable C2 systems increase a commander's warfighting capabilities since every aspect of the operation depends heavily on the vital flow of essential information.

The Problem

The inability to effectively communicate (i.e., exchange information) among the military service systems is thoroughly documented in operational after action reports and well-publicized by Congressional inquiries into command and control failures.[6] The blame for this problem tends to focus on the

incompatibilities that exist between the military service communications equipments, their automated and manual operating procedures, and their poorly defined C2 architectures. Near term solutions primarily involve inserting technical fixes between system components using combinations of unique interface, buffering or translative devices. These devices are expensive and become more inefficient as the number of interacting, dissimilar systems increase. In fact, every "break" in the system where information must be decoded, converted, translated, and encoded slows down the timeliness in flow and can create errors in the data.

The lack of a common joint C2 architecture and operational doctrine has hindered getting the military services to coordinate their system developments. Joint efforts such as the Tri-Service Tactical Communications (TRI-TAC) program to provide a joint common-user, tactical switching and backbone communications network; the Joint Interoperability of Tactical Command and Control Systems (JINTACCS) program to develop common digital data links and message formats; and the Joint Tactical Information Distribution System (JTIDS) program to distribute computer data across the battlefield, fell short of their goals to achieve complete interoperability.[7] Some capabilities derived from these three programs have contributed to a partial joint C2 architecture, but manual versus automated interfaces, different service communications support systems, and service disagreements on an information processing and distribution scheme are symptomatic of the bureaucratic barriers to achieving

interoperability.

Congress inititated efforts to reduce these barriers. The Defense Reorganization Act of 1986 with its emphasis on "jointness" gave the Chairman, Joint Chiefs of Staff (CJCS) the authority to stifle interservice rivalries, articulate joint requirements, and encourage the military services to cooperate toward using common equipments. Tightening fiscal realities also dictate on how a service will meet its needs by making it economize on "joint" vice service-unique solutions. Further, the Joint Tactical Command, Control, Communications Agency (JTC3A) has been developing functional interoperability architectures (FIA) for each combatant theater; these will clearly show how, where, and when information exchange requirements occur within and across functional areas between command and control elements. And recently, the Joint Requirements Oversight Council (JROC) of the Joint Staff reported the results of a study on Joint Tactical Fusion Interoperability (JTFI) that appears to pinpoint the problem.

> After a thorough examination of the issues, the JTFI Steering Group concludes that interoperability of JTF systems and, by extension, all C3I systems has been impeded by the absence of defined, coordinated, and enforced telecommunications, information, and information processing standards. The absence of a unified set of interoperability standards is caused largely by the fragmentation of responsibility for standards at the OSD level.
>
> The absence of a centralized management structure for C3I standards results in the proliferation of C3I systems which are not interoperable or may only be interoperable after extensive development and maintenance of translation devices.[8]

This finding reveals what may very well be the root cause of interoperability problems.

Common Standards

Interoperability is more than just a perfect telecommunications system. Both information and information processing also must be included. An objective technique to best describe and evaluate C2 systems interoperability was constructed by Major John Woodward USMC during the Joint Tactical Fusion (JTF) study efforts. His model incorporates the three essential components found in all systems: **inputs and outputs**, a **path** over which those inputs and outputs travel, and a **process** that supports the system's specific function.[9] **Inputs and outputs** are comprised of <u>information</u> in various forms, i.e., data files, message text formats, digitized maps, security classifications, imagery and display symbology/graphics. The **path** is the means to <u>transmit</u> the information. It can be telecommunications networks using appropriate protocols, encrypted radio links, or wire/fiber optic systems, or signal flags, lights, messenger or some combination of each. The **process** is <u>information processing</u>, i.e., the action done on inputs to produce an output. Processing can be message parsing, correlation algorithms, modeling or even a human processor.[10]

The concept for this model is to follow the flow of information through the system to illustrate where the obstacles to interoperability occur. For example, data element (<u>information</u> component) for date and time should be standard for the process (<u>information processing</u> component) to calculate items

such as elapsed time, time available on-station, conversion of universal date/time to local date/time or other uses, even though it may be displayed in several different formats. That information should also be capable of being passed (telecommunications component) to another system or database which can readily accept it. It so happens that numerous date/time formats in lengths from 7 to 14 alphanumeric characters presently exist in various C2 databases; hence, they are not easily transmitted or processed between different systems. Examples of two other data elements with duplicate standards are aircraft type which ranges in format length from 1 to 6 characters or symbols, and the data element for radio frequency which ranges in format length from 3 to 16 alphanumeric characters or symbols.[11] Many data elements (information) are unique in the various military operational, intelligence, manpower, financial and logistics database systems which support C2. The direct exchange of data elements through the C2 system model is inhibited when the various conventions and formats used to define them cannot be accepted and processed by each system component.

Standardization of the C2 systems components varys in many ways without regard to fitting into a larger system. To fully standardize a system, each of the three components; telecommunications, information, and information processing, must adhere to common standards, the basis of interoperability. The long-term solution is to design and develop all C2 system components for universal interoperability. Current system developments are frequently designed to support only one functional

area requirement; i.e., they fit into a stovepipe information flow. This is quite prevalent with intelligence systems. Even though they have information of interest usable by tactical fire and maneuver and air operations systems, technical and procedural barriers exist based on unique functional system standards. Three specific examples illustrate current interoperability problems where service preferences in information formats and equipments differ.

> 1. Digital Entry Devices (DED) are terminals for burst transmission of tactical data over voice radio nets and switched cable systems to pass free text or formatted messages to request artillery fire, close air support or other tactical functions. DEDs were purchased by all the services, but cannot exchange data between themselves because each service uses different communications protocols and/or different types of message formats.[12]
>
> 2. Secondary Imagery Dissemination Systems (SIDS) are used for transmitting digital imagery from national sources to operational units. Of the five SIDS and one secure facsimile system now in use by tactical forces, only one system interoperates with more than one other SIDS. Both common communications and data protocols are necessary to establish basic interoperability between these type systems.[13]
>
> 3. The US Transportation Command must integrate over 110 automated data processing (ADP) systems into a global transportation network to be able to rapidly plan, coordinate, and direct strategic airlift and sealift assets worldwide. There is no data standardization in format, content, and definition for the same information elements across many of these systems. The lack of a single set of standards impairs this effort.[14]

The idea to establish common communication, information (data) and information processing structures will allow multiple users to efficiently access, process, and share data between distributed ADP networks using common telecommunications networks. The ability to integrate different hardware and software products will exist when vendors provide Open Systems Interconnection (OSI) features into their system interfaces as defined by the Government Open Systems Interconnection Profile (GOSIP) standard. This concept presses the issue of integrating warfighting C2 systems and non-tactical automated (business-type) information systems (AIS). Although information sharing between these two realms is hindered by security procedures and stringent environmental survival considerations, the development of common data standards for exchanging their information should be initiated now.

Note that the following sections will refer to "C2 systems" as "C3I systems" to conform to official organization titles and the practice by DOD and the Joint Staff to highlight the role of communications and intelligence in command and control.

Current Structure

"Centralized management and coordination of standards are required to improve upon the morass of fragmented, inconsistent, and ineffective standards now in effect."[15] This revelation has slowly evolved over the last two years as different DOD interoperability fora have investigated development, acquisition, and operational issues between service systems. The JTFI Steering Group (JTFISG) is a senior-level formal oversight committee

to act on interoperability issues among joint tactical fusion (JTF) systems and C3I systems at the theater, national, and allied levels.[16] The early work of this group under JROC tasking was instrumental in identifying the root causes in achieving interoperability between JTF systems. It also revealed deficiencies in current organizational management structures on standards. A major finding was that JTF is considered a subset of C3I.

The group was initially tasked to evaluate interoperability among certain JTF systems; the Army All-Source Analysis System (ASAS), the Air Force Enemy situation Correlation Element (ENSCE), the Navy Intelligence Support to Strike and Amphibious Forces (ISS/AF) project, and the Marine Corps Technical Control and Analysis Center (TCAC). During their investigation, they discovered some key deficiencies in JTF management. No commonly accepted nor jointly approved definitions existed for fusion, tactical fusion or joint tactical fusion; nor was there as single DOD or Joint Staff organization designated for JTF management and oversight. Hence, organizations charged to act on C3I capabilities had no definitional reference to believe JTF should be included in C3I.

A proposed definition of fusion and an expanded definition of the term "joint" were the first steps in determining management responsibility. Fusion is defined as: "a machine-aided data reduction process for integrating reports from all available and appropriate sources (friendly and enemy) to develop a coherent display of a commander's area of interest to assist in

C3I functions."[17] Although JTF is more than just the fusion of intelligence information; the intelligence community constitutes most of the nation's fusion capabilities. Therefore, for JTF, the term joint needs to also include the role of agencies like the Defense Intelligence Agency (DIA) and National Security Agency (NSA) as additions to the two or more services condition.

JTF is an automated decision support mechanism which both supports the execution of C3I and is supported by C3I systems. This involves ADP, connectivity, and compatibility among communications and ADP systems, establishing standards of interoperability, and tailoring developments to meet theater commanders and services requirements. A commander's C2 system helps him see-decide-act as discussed earlier in this paper; a JTF system enables him to see the battlefield and gather needed information in near-realtime to decide on his action inside the enemy commander's decisionmaking cycle. Multiple sources and sensors provide through the C3 system, intelligence and operational information for the JTF system to process, integrate, store and display (i.e., fuse) for the commander to use in making operational decisions.[18]

It was this close relationship between JTF and C3I that justified the Vice Chairman, JCS to designate the Director, C3 Directorate (J-6), Joint Staff, as JTF lead. He is supported by the JTFISG which he chairs. Members include general or flag officer (O-7/O-8) and Senior Executive Service (SES) equivalent representation from the DIA, NSA, Defense Communications Agency (DCA), Joint Staff Operations (J-3), Logistics (J-4), Operational

Plans and Interoperability (J-7), and Force Structure, Resource, and Assessment (J-8) Directorates, JTC3A, each military service, and the Defense Mapping Agency (DMA). An Intelligence Community (IC) Staff and Assistant Secretary of Defense C3I SES advisor or observer are invited at the call of the Chairman.[19]

The next significant situation the study group revealed was that DOD C3I policy and the companion JCS Memorandum of Policy on interoperability were too limited in scope to permit full integration of C3 processes with intelligence processes. DOD Directive 4630.5, Compatibility and Interoperability of Command, Control, Communications, and Intelligence Systems, restricted the treatment of interoperability between C3 and intelligence systems to only interfaces.[20] This allowed the C3 and intelligence communities to develop separate standards that serve their own needs rather than an integrated C3I function. Consequently, this lack of standard specifications for C3I severely hindered the automated fusion of intelligence and operations data. Although this policy directive talks to "C3I" throughout the document, it doesn't task any intelligence activity as the lead with specific responsibilities, and by omission, excludes their participation in the C3 Review Council.[21] In fact, there is no "C3I" forum established. The two communities are together by name, but separate by action.

The JCS policy, Compatibility and Interoperability of Tactical Command, Control, Communications, and Intelligence Systems (JCS MOP 160) suffers the same limitations as the DODD 4630.5. It lacks direction for DIA responsibilities in its role

as the Joint Staff J-2, and relegates C3I interoperability responsibilities to JTC3A.[22] This is particularly significant since JTC3A is charged with developing and maintaining the joint tactical "C3" architecture. Intelligence clearly needed to be integrated into that document. It is further responsible for end-to-end system testing of computer/communications networks.

In looking at the way ahead to formally integrate the organizations that work intelligence with those that work C3, the JTFISG determined that the coordination and establishment of a family of C3I interoperability standards was urgently needed. It was further discovered that standardization programs and guidance already existed within DOD, but were not followed. The Assistant Secretary of Defense for Production & Logistics (P&L) through his subordinate Defense Quality and Standardization Office (DQSP) is responsible for administering the single, integrated Defense Specification Standardization Program (DSSP) for DOD.[23] The DSSP has 34 technology standardization areas which include communications standards managed by DCA/JTC3A and information processing standards for computers (IPSC) for general purpose computers managed by Headquarters, US Air Force.[24] ASD (P&L) is also responsible for the DOD Configuration Management (CM) Program which applies to most computer and communications equipments.[25]

The DOD Comptroller directs and controls the Data Elements and Data Codes Standardization Program. This program facilitates data interchange and compatibility among DOD data systems that "support such functions as command and control, logistics,

intelligence, personnel, and financial management."[26] The comptroller is responsible for the management of computer resources in major and non-major defense systems, i.e., mission critical computer resources (MCCR) that are acquired as integral to systems supporting intelligence, cryptologic, and C2 activities, and weapons.[27] He also manages the DOD Information Resources Management (IRM) program which primarily concerns the sharing, storing, and reporting of non-tactical information.[28]

Another concurrent executive level study group discovered similiar discrepancies in information systems standards management while preparing a plan for Corporate Information Management (CIM) for DOD. The CIM concept is a business-oriented approach to use information system computing and communications technology to implement new solutions to old problems in order to achieve dramatic improvements in business efficiencies and effectiveness.[29] Several principles which guide this concept parallel the interoperability conditions for C2 systems.

1. Information will be managed through centralized control and decentralized execution.

2. Information systems performing the same function must be common unless specific analyses determine they should be unique.

3. The computing and communications infrastructure will be transparent to the information systems that rely upon it.

4. Common definitions and standards for data will exist DOD-wide.

5. Data will be entered only once.[30]

Their analysis of DOD information management and technology revealed symptoms similar to the C2 systems interoperability issues.

> 1. Information Management
>
> A. Responsibilities for information management are fragmented within DOD.
>
> B. Standardization of data across the Department has not yet been achieved, and most data continues to be managed in separate, functional "stovepipes."[31]
>
> 2. Information Technology
>
> A. The Department's technology base has evolved into a variety of disparate computing and communications architectures. The effectiveness of new technology system developments is limited because of interoperability problems with existing systems.
>
> B. The Department has a multiplicity of unique information system architectures with incompatible hardware, software, and communications networks.
>
> C. The lack of uniform standards within the Department has contributed to incompatible data and systems, and has impaired the ability to exchange information among systems or users, port systems to new architectures, interface with allies, or take advantage of commercial products.
>
> D. Communications gateways are frequently required between systems to achieve interoperability or data exchange without human intervention.
>
> E. Information systems are operated with a variety of unique user interfaces.[32]

It is evident that common standards for both tactical and non-tactical information systems have not been adequately implemented nor managed within DOD. It is certainly clear that no central authority coordinated the development of C3I standards as computing and communications technology rapidly advanced our capabilities to exchange information with each other faster, more clearly, and over longer distances. It appears that the high-

level policies and programs of ASD (P&L), DOD (C) and ASD (C3I) should have effectively been able to allow for the coordination and integration of common standards for C3I system components.

Assessment

The systemic interoperability problem requires a top-down management vice a bottom-up technical solution. Top management must clarify and coordinate their responsibilities to institute an effective interoperability program. The three principal OSD executives having key central management responsibilities are ASD (P&L), DOD Comptroller, and ASD (C3I). Lets look at how their responsibilities relate and intersect.

ASD (P&L) functions under the direction, authority, and control of the Under Secretary of Defense for Acquisition (USD(A)). This office provides the overall management policy for DOD Configuration Management (CM) practices. CM applies throughout the life cycle of configuration items (CI) in major and non-major defense systems, and specifically includes computer hardware, firmware, and software. CM also encompasses a CIs joint and combined tactical C3I interoperability characteristics.[33] All DOD components are responsible to manage the configurations of their C2 and information systems under this program. The Defense Quality and Standardization Office (DQSP) under ASD (P&L) is responsible for administering the DSSP to achieve the optimum degree of uniformity among items, materials, and engineering practices in all phases of the life cycle of systems and equipments developed or used by DOD.[34] This office assigns specific management responsibilities to

primary services and DOD agencies for their discrete functional area standards. The C3I concept was synthesized well after the 1979 implementation of DSSP, and has relied on individually managed functional components; the provisions of DSSP to manage C3I standards apply under DOD Directive 4120.3. DQSP also resolves any conflict with national and international standards or standardization agreements.[35] ASD (P&L) chairs the Defense Standardization Council (DSC) chartered to develop standardization policies under the DSSP. The DOD Comptroller is a permanent member and, when required for telecommunications issues, the ASD (C3I) attends.

The DOD Comptroller has been responsible to direct and control the Data Elements and Data Codes Standardization Program and monitor its application by DOD components since 1964. The program applies to all DOD components concerned with the development and use of data systems which support such functions as command and control, logistics, intelligence, personnel, and financial management. Cryptologic activities are exempted. The policy and program implementing instructions (DOD Directives 5000.11, 5000.11-M, & 5000.12) do not refer to the DSSP, although the comptroller is a member of the DSC. Like the DSSP, this program is similarily decentralized throughout DOD among assigned responsible agents (ARA) tasked to manage their area of data standards.[36] The following list identifies the current ARAs and data standards areas:

DOD (C) -DOD Resources Management Systems
-Organization Identification
-Special Circumstances
-Time

ASD (P&L)	-Quantitative
DCA	-Defense Communications System
DIA	-Intelligence -Geopolitical -Security
JCS	-World Wide Military C2 System (WWMCCS) --National Military Command System --U&S Command C2 systems --Tactical C2 systems -Joint Comm-elec Operating Methods and Procedures
Army	-Central Index of DOD Investigations -Language -Survival Measures
Navy	-Civilian Personnel -Configuration Management -Military Personnel (except CIVPERS; JUMPS)
Air Force	-JUMPS -Judge Advocate General -Medical and Dental

As can be seen by the above list, area assignments lack comprehensive coverage. The program reflects concepts and procedures applicable during the mid-1960s, and it has not been updated since its inception. The program lacks an enforcement mechanism; hence, little standardization of data elements has been accomplished. This program needs to be revitalized and expanded.

The DOD Comptroller is also responsible for the policy and guidance for MCCR (tactical) and IRM (includes AIS; i.e., non-tactical) programs in that the computer resources in each program are acquired under different federal procurement regulations. Life cycle management (LCM) of AIS is to ensure that appropriate interoperability requirements are included in the functional

requirements and the system design of new AISs and the modernization of existing AISs. DOD (C) establishes the LCM policy and tasks ASD(C3I) to develop policies and issue guidance to DOD components for the development, acquisition, implementation, and operational use of telecommunications and computer security systems for all DOD AIS. The program allows each DOD component to establish procedures for exemptions from the use of applicable Federal Information Processing Standards (FIPS), although FIPS and federal standards shall be relied upon and in their absence, DOD and military standards shall be relied upon whenever possible.[37] Both programs invoke compliance with the Data Standardization Program (DOD Directive 5000.11) and CM program (DOD Directive 5010.19). The IRM program delegates execution to DOD components. There is no stated requirement for systems interoperability. This program tends to support an independent, bottoms-up procurement approach to automate existing manual ways of doing business. Funds control vice information management is the probable rationale why the comptroller is tasked to monitor and manage these programs.

ASD (C3I) is the principal DOD staff advisor for all matters relating to C3I policy, requirements, priorities, systems, resources, and programs to include DOD warning and reconnaissance programs. This office recommends, advises, and provides assistance to other staff agencies on C3I matters relevant to the execution of their assigned responsibilities which include implementing DOD-wide programs to improve standards of performance, economy, and efficiency.[38] He is functionally

responsible for strategic, theater, and tactical C2 systems; telecommunications; application and integration of ADP technology; surveillance, warning, and reconnaissance architectures and systems to support C3I activities; and the integration of national and tactical C3I. He exercises direction, authority, and control over DCA, JTC3A, Defense Mapping Agency (DMA), DIA, and the General Defense Intelligence Program (GDIP) staff.[39] Staff supervision is exercised over NSA and service communications and intelligence activities. Excluded from ASD(C3I) control are C3 systems which are integrally designed into weapon systems. ASD(C3I) chairs the C3I Systems Committee when preparing advice, assistance, and recommendations to the USD(A) Defense Acquisition Board (DAB) regarding C3I systems acquisition issues.[40] He also chairs the C3 Review Council, a senior-level forum to resolve C3 compatibility and interoperability issues, or prepare recommendations for the C3 Executive Committee, chaired by the Deputy Secretary of Defense.[41] Both of these forums have been inactive over the past three years.

On 16 November 1990, the Secretary of Defense designated ASD(C3I) as the DOD Information Management Official and assigned him the responsibility for establishing an organization to implement CIM throughout DOD, and the authority for ensuring the proper integration of DOD computing, telecommunications, and information management activities.[42]

Conclusion

The most significant point for the Defense, Service and Agency C3I communities and, in fact, for the whole Defense Department, is to recognize that standards are the foundation in which to begin providing interoperable C3I systems. The first step toward achieving interoperability is to gain the total commitment and daily support of these communities to develop, abide by, and maintain C3I standards. Secretary Cheney recognized the importance of the ASD(C3I) functions to DOD when he centralized the authority for Corporate Information Management and information management. This has essentially established ASD(C3I) as the single DOD authority for C3I standards.

In assuming this responsibility, ASD(C3I) must clarify and resolve areas of overlapping responsibility between the DOD Comptroller and ASD(P&L), and implement the policy that makes interoperability and the application of approved standards mandatory in the acquisition of future AIS and C3I systems. Understandings and relationships between C3 and intelligence activities must also be formalized into the daily routine, and C3 coordinating councils should be expanded to include intelligence as a permanent participant.

The data standardization program for data elements and codes needs to be revitalized and updated into a broader program that will allow system developers to build information systems that can share data with many other systems. It must follow life cycle management and configuration management practices and operate under the umbrella of the Defense Standardization and

Specification Program. A standards management structure must be instituted to provide a permanent, focused, and consistent process for program and functional managers to coordinate and resolve interoperability issues. It can be organized on the three C2 systems components; information (data), information processing, and telecommunications; and built upon existing organizations and committees while expanding them or adding new groups, as required.

Enforcement of standards is critical to ensure program compliance. Existing test and evaluation mechanisms need to clearly understand the standards and techniques needed to validate and verify performance. Test results must substantiate that the system meets interoperability requirements and is in compliance with approved standards. This interoperability certification must be validated at each appropriate milestone decision point or program review. All C2 systems and AIS must be reconciled against valid requirements that are reflected in thoroughly developed national, theater, and functional interoperability architectures. These baseline documents must be under strict configuration management as they are the essential diagrams of information exchange requirements.

The only way to effectively solve interoperability problems is to start from the top. The bureaucratic barriers, organizational self-interests, and isolated functional orientations to developing systems can only be overcome by a top-level authority who implements a centrally managed structure to coordinate and guide operators and developers in creating

effective and efficient C2 and information systems on common information, information processing and telecommunications standards, the basis of interoperability.

ENDNOTES

1. Ronald C. Bethmann and Karen A. Malloy, Command and Control: An Introduction, p. 18.

2. Joint Publication 1-02, Dictionary of Military and Associated Terms, p. 77 (hereafter referred to as "JPub 1-02").

3. Bethmann, p. 19.

4. John Woodward and Doug Lynn, "C2 Systems Interoperability," Amphibious Warfare Review, Summer 1990, p. 53.

5. JPub 1-02, p. 190.

6. U.S. General Accounting Office, DOD's Efforts to Achieve Interoperability Among C3 Systems, p. 8.

7. Ibid., p. 21.

8. Joint Requirements Oversight Council Memorandum (JROCM) 073-90, C3I Systems Interoperability, p. 1.

9. Woodward, p. 54.

10. Ibid.

11. Ibid., p. 55.

12. Hunter Dixon, "Joint Tactical Fusion Interoperability," JROC Briefing, p. B-1.

13. Ibid., p. B-2.

14. Ibid., p. B-3.

15. Department of the Navy Memorandum, Interoperability of Command and Control Systems, pp. 1 and 2.

16. Director, Joint Staff Memorandum 727-89, Joint Tactical Fusion Lead and Interoperability, attachment, p. 1 (hereafter referred to as DJSM-727-89).

17. Joint Requirements Oversight Council Memorandum (JROCM) 009-89, Joint Tactical Fusion Interoperability, p. I-1.

18. Ibid., p. II-A-3.

19. DJSM-727-89.

20. DOD Directive 4630.5, Compatibility and Interoperability of Tactical Command, Control, Communications, and Intelligence Systems, p. 1.

21. Ibid., pp. 1 and 6.

22. JROCM-009-89, p. IV-1.

23. DOD Directive 4120.3, Defense Standardization and Specification Program, p. 1.

24. DOD Directive 7740.1, DOD Information Resources Management, p. 1-4.

25. DOD Directive 5010.19, DOD Configurstion Management Program, p. 1.

26. DOD Directive 5000.11, Data Elements and Data Codes Standardization Program, p.1.

27. DOD Directive 5000.29, Management of Computer Resources in Major and Non-major Defense Systems, p. 1.

28. DOD Directive 7740.1, p. 1.

29. Office of the Secretary of Defense Memorandum, Corporate Information Management, p. 1.

30. Ibid., p. 3.

31. Ibid., pp. 15 and 16.

32. Ibid., pp. 18 and 19.

33. DOD Directive 5010.19, p. 2.

34. DOD Directive 4120.3.

35. Assistant Secretary of Defense for Production and Logistics Memorandum, JTFISG Report to the Joint Requirements Oversight Council, p. 2-3.

36. DOD Directive 5000.12, Data Elements and Date Codes Standardization Procedures, p. 1.

37. DOD Directive 7920.1, Life Cycle Management of Automated Information Systems, pp. 6 and 7.

38. DOD Directive 5137.1, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, p. 1.

39. Deputy Secretary of Defense Memorandum, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, p. 1.

40. DOD Instruction 5000.2, Defense Acquisition Program Procedures, p. 2.

41. Deputy Secretary of Defense Memorandum, Charter for C3 Review Committee, p. 1.

42. Secretary of Defense Memorandum, Implementation of Corporate Information Management Principles, p. 1.

BIBLIOGRAPHY

Allard, C. Kenneth. Command, Control, and The Common Defense. New Haven: Yale University Press, 1990.

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum. Joint Tactical Fusion Interoperability (JTFI) Steering Group Meeting on 1 June 1990. Washington: OSD, 23 August 1990.

Assistant Secretary of Defense for Production and Logistics Memorandum. JTFISG Report to the Joint Requirements Oversight Council (JROC). Washington: DQSO, 12 October 1990.

Bethmann, Ronald C., and Malloy, Karen A. Command and Control: An Introduction. Thesis. Monterey: U.S. Naval Postgraduate School, March 1989.

Cushman, John H. "Joint Command and Control," Military Review, Vol. 70, July 1990, pp. 25-34.

Deputy Secretary of Defense Memorandum. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. Washington: OSD, 27 November 1990.

Deputy Secretary of Defense Memorandum. Charter for C3 Review Committee. Washington: OSD, 3 November 1983.

Director Joint Staff Memorandum 727-89. Joint Tactical Fusion Lead and Interoperability Steering Group. Washington: Joint Staff, 19 June 1989.

Dixon, Hunter, LTC. "Joint Tactical Fusion Interoperability," JROC Briefing. Washington: DIA/CS-2B, 25 October 1990.

Department of Defense Directive 4120.3. Defense Standardization and Specification Program. Washington: USDR&E, 10 Feb 79.

Department of Defense Directive 4630.5. Compatibility and Interoperability of Tactical Command, Control, Communications, and Intelligence Systems. Washington: ASD(C3I), 9 Oct 85.

Department of Defense Directive 5000.1. Major and Non-major Defense Acquisition Programs. Washington: USD(A), 1 Sep 87.

Department of Defense Instruction 5000.2. Defense Acquisition Program Procedures. Washington: USD(A), 1 Sep 1987.

Department of Defense Directive 5000.3. Test and Evaluation. Washington: USDRE, 12 March 1986.

Department of Defense Directive 5000.11. Data Elements and Data Codes Standardization Program. Washington: ASD(Comp), 7 December 1964.

Department of Defense Directive 5000.12. Data Elements and Data Codes Standardization Procedures. Washington: ASD(Comp), 2 April 1985.

Department of Defense Directive 5000.18. Implementation of Standard Data Elements and Related Functions. Washington: ASD(Comp), 17 March 1969.

Department of Defense Directive 5000.29. Management of Computer Resources in Major and Non-major Defense Systems. Washington: ASD(Comp), 16 May 1989.

Department of Defense Directive 5010.19. DOD Configuration Management Program. Washington: ASD(P&L), 28 Oct 1987.

Department of Defense Directive 5105.19. Defense Communications Agency. Washington: ASD(A&M), 12 December 1988.

Department of Defense Directive 5134.1. Under Secretary of Defense for Acquisition. Washington: USD(A), 8 Aug 1989.

Department of Defense Directive 5137.1. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. Washington: ASD(C3I), 2 April 1985.

Department of Defense Directive 7740.1. DOD Information Resources Management Program. Washington: ASD(C), 20 June 1983.

Department of Defense Directive 7920.1. Life Cycle Management of Automated Information Systems. Washington: ASD(C), 20 June 1988.

Department of the Navy Memorandum. Interoperability of Command and Control Systems. Washington: CNO/CMC C2IO, 28 March 1990.

Department of the Navy Program Budget Decision 924. ADP Consolidation. Washington: DON, 13 NOvember 1990.

Dordal, Paul R., LtCol. An Appraisal of the Joint Tactical Fusion Program (JTFP): Will the JTFP Provide Interoperability Requirements for Successful Joint Operations? MPS. Carlisle Barracks: U.S. Army War College, 4 April 1990.

Dyer, Herbert D., LTC. Joint Tactical Command, Control and Communications (C3) Interoperability. MSP. Carlisle Barracks: U.S. Army War College, 12 March 1990.

Joint Chiefs of Staff Memorandum of Policy (MOP) 160. Compatibility and Interoperability of Tactical Command, Control, Communications, and Intelligence Systems. Washington: JCS, 7 June 1986.

Joint Publication 1-02. DOD Dictionary of Military and Associated Terms. Washington: USGPO, 1 Dec 1989.

Joint Publication 6-0 (Test Pub). Doctrine for Command, Control, and Communications Systems Support to Joint Operations. Washington: J-7, 12 June 1990.

Joint Requirements Oversight Council Memorandum 009-89. Joint Tactical Fusion Interoperability. Washington: JCS, 1 March 1989.

Joint Requirements Oversight Council Memorandum 073-90. C3I Systems Interoperability. Washington: Joint Staff, 14 November 1990.

Kahan, James P.; Worley, D. Robert; and Stasz, Cathleen. Understanding Commanders' Information Needs. Santa Monica: Rand Corporation, June 1989.

Office of the Secretary of Defense, Special Assistant Memorandum. Corporate Information Management. Washington: 6 Nov 1990.

Olszewski, Robert V. "C3I Interoperability," Sperry, Vol. 9, November-December 1983, pp. 2-11.

Secretary of Defense Memorandum. Implementation of Corporate Information Management Principles. Washington: OSD, 16 November 1990.

Snyder, Frank M. Command and Control Readings and Commentary. Cambridge: Harvard University, April 1989.

U.S. Department of Defense. DEFENSE 90 Almanac. Washington: USGPO, November-December 1990.

U.S. Department of Defense. Organization and Functions Guidebook. Washington: OSD(OMP), February 1990.

U.S. General Accounting Office. Battlefield Automation: Army Tactical Command and Control System's Cost and Schedule. Washington: GAO-NSIAD-90-28BR, 8 Feb 1990.

U.S. General Accounting Office. DOD's Efforts to Achieve Interoperability Among C3 Systems. Washington: GAO/NSIAD-87-124, 27 April 1987.

U.S. General Accounting Office. Navy Command and Control: Data Fusion Needs and Capabilities for Battle Group Commanders. Washington: GAO/NSIAD-90-69BR, 7 March 1990.

Van Creveld, Martin. Command in War. Cambridge: Harvard University Press, 1985.

Woodward, John, Maj USMC, and Lynn, Doug, CDR, USN. "C2 Systems Interoperability," Amphibious Warfare Review, Summer 90, pp. 52-56.