# The Challenges Associated with Achieving Interoperability in Support of Net-Centric Operations

**Dr. Stuart H. Starr**
**Barcroft Research Institute**
**Falls Church, VA 22041**

**e-mail: stuartstarr@cox.net**

**Abstract**

Recently, John Stenbit, former ASD(NII), articulated his views on the keys to achieving effective Net-Centric Operations (NCO) (Reference 1). As the foundation for this capability, he called for the creation of a ubiquitous, secure, robust, trusted, protected and routinely used wide-bandwidth net that is populated with the information and information services that our forces need. Furthermore, he observed that we must move from a set of monopoly suppliers of information to an information marketplace; from a push-oriented dissemination process to a pull-oriented one; and from an interoperability approach based upon applications standards to one based upon data standards (where an unanticipated user can find, access, and use data, anywhere, anytime). This vision requires us to critically reassess the nature of the interoperability problem.

To illuminate the issue, this paper addresses three inter-related dimensions of the interoperability problem. First, it characterizes the nature of the interoperability issue. This includes consideration of the questions: What is interoperability? How is interoperability currently achieved? Why is it difficult to achieve interoperability of IT systems? How are we doing in achieving interoperability? Second, it identifies key longer-term trends and derives interoperability implications. These trends include potential changes in the areas of geopolitics, national security, strategic vision, institutional initiatives, systems, technology, and testbeds. Finally, it identifies and discusses residual interoperability challenges that the community must address in five areas: institutional, program management, architectures and standards, operational, and systems.

Emphasis is placed on interoperability among $C^4I$ systems in the context of joint, interagency, multinational (JIM+) net-centric operations, where the "plus" refers to additional participants such as international organizations (e.g., the United Nations), non-governmental organizations (NGOs) (e.g., Doctors Without Borders), and contractors.

## 1. Introduction

Achieving information technology (IT) interoperability is one of the most challenging and important issues confronting the defense community. Interoperability is the foundation for critical Command, Control, Communication, Computer, and Intelligence ($C^4I$) systems. The Chairman, Joint Chiefs of Staff (CJCS), in Joint Vision 2020 (Reference 2) placed this issue front and center in his priorities. Joint Vision 2020 articulates a vision of a future "system of systems" that exploits the enormous potential of net-centric operations. This vision explicitly requires substantial improvements in $C^4I$ interoperability. To illuminate the issue, this paper has three foci:

• to characterize the nature of the interoperability problem;
• to describe recent initiatives to ameliorate interoperability shortfalls; and
• to identify and discuss interoperability challenges.

Emphasis is placed on interoperability among $C^4I$ systems in the context of joint, interagency, multinational (JIM+) operations, where the "plus" refers to additional participants such as international organizations (e.g., the United Nations), non-governmental organizations (NGOs) (e.g., Doctors Without Borders), and contractors.

# 2. Nature of the Problem

## 2.1 What is Interoperability?

Considerable confusion exists over the meaning of the term interoperability. Many definitions are in use and they are sometimes inconsistent in their scope and detail. As a point of departure, systems are interoperable if they have two key factors in common. They allow units to exchange data in a prescribed manner, and they use the extracted information to operate together effectively. The imperative to automate this exchange is driven by the desire to reduce delays in distributing information and to expand the amount of information that can be transmitted.

Furthermore, commanders of JIM+ operations emphasize that data exchanged must be sufficiently complete, accurate, and timely to be consistent with the needs of the operation being supported. In addition, the definitions imply that interoperability is not a binary variable. In fact, many gradations of interoperability exist in systems that have been fielded.

In view of the ambiguity associated with the term interoperability, four complementary perspectives of the term are presented below. Each of the perspectives emphasizes a unique aspect of the problem with which we are confronted.

### 2.1.1 Levels of Interoperability: An Operational Perspective

At one extreme, there are many instances of organizations that must exchange information in a timely manner, yet possess separate and independent systems that are totally non-interoperable. This limits information exchange to purely manual means (e.g., by ancillary voice or teletype communications).

At the next level of interoperability, limited numbers of liaison teams may be exchanged along with their systems to affect a limited exchange of information. This is representative of the approach that was implemented among selected allies in Operation Allied Force in the Balkans.

At a third level of interoperability, the concept of "swivel chair" interoperability has emerged. In this approach, an operator implements the exchange of information by manually accessing two systems that would otherwise be non-interoperable and acting as an interpreter. In this instance, the human can be under considerable pressure and is prone to limit the capacity and accuracy of the information exchanged. For example, during Operation Iraqi Freedom, some Marines had to use two laptops, a helmet headset, and four radios simultaneously to communicate with their commanders and other units.

At a fourth level of interoperability, two systems are given restricted, automated interoperability by providing them with a subset of common modes that can be properly processed by both. However, in this approach, it is not unusual to have austere common modes (e.g., modes that lack resistance to enemy countermeasures and possess limited processing capacity). A variant of this involves implementing automated gateways to support the limited exchange of information between systems. The extent of interoperability is driven, in large part, by the consistency of the standards and protocols selected for the two systems' communications-

processing layers. Frequently, these interfaces are restricted by security or operational considerations.

Finally, there is a level of interoperability at which two systems are capable of accurately exchanging all relevant data, automatically, with time scales and capacities consistent with operational needs. Currently, very few examples exist where such levels of interoperability have been achieved.

These levels of interoperability suggest a broad trend in the desired evolution of $C^4I$ systems. Originally, $C^4I$ systems were largely manual, and interoperability, if it existed at all, was achieved through manually intensive techniques. Currently, $C^4I$ systems are becoming more automated and there is considerable interest in developing automated interfaces that impose fewer restrictions on the timely, accurate, and comprehensive exchange of information. As discussed below, the level of automation to achieve interoperability for a particular set of systems depends strongly on the benefits and liabilities associated with alternative levels of implementation.

### 2.1.2 The "Integration Continuum"

Recently, RADM Robert Nutwell (USN, ret) defined three key terms: integration, interoperability, and compatibility (Reference 3). He distinguished among those terms as follows:

- "Integration is generally considered to go beyond mere interoperability to involve some degree of functional dependence (e.g., … an air defense missile system will normally rely on an acquisition radar)… An integrated family of systems must of necessity be interoperable, but interoperable systems need not be integrated."
- "Compatibility … means that systems/units do not interfere with each other's functioning. Interoperable systems are by necessity compatible, but the converse is not necessarily true."
- "In sum, interoperability lies in the middle of an 'Integration Continuum' between compatibility and full integration."

### 2.1.3 Domains of Warfare

A recent monograph on net-centric operations by Alberts & Hayes identified four domains of warfare (Reference 1):

- Physical domain, where strike, protect, and maneuver take place across different domains;
- Information domain, where information is created, manipulated, and shared;
- Cognitive domain, where perceptions, awareness, beliefs, and values reside and where, as a result of sensemaking, decisions are made; and
- Social domain, characterizing the set of interactions between and among force entities.

Alberts & Hayes argue that to support net-centric operations effectively, a high level of interoperability must be achieved within and across each of these domains. This perspective emphasizes the critical problem of achieving meaningful interoperability when the individuals involved come from different cultures (e.g., speak different languages, employ different concepts of operations).

### 2.1.4 Levels of Information Systems Interoperability (LISI): A Systems Perspective

This perspective of interoperability is closely aligned to the five levels of interoperability introduced in section 2.1.1. It was generated to provide a reference model and process for assessing interoperability between and among information systems (Reference 4). The LISI model also specifies five levels of interoperability (ranging from levels zero to four) as depicted

in Table 1. It distinguishes among alternative levels and treatments of procedures, applications, infrastructure, and data. As such, it adopts a perspective that is reflective of the viewpoints of a computer scientist/system engineer. Recent initiatives are seeking to build upon this framework to provide a structured and systematic approach for assessing and measuring interoperability throughout the system life cycle (Reference 5).

**Table 1. LISI Taxonomy**

| Level | Description | Procedures | Applications | Infrastructure | Data |
|---|---|---|---|---|---|
| 4 | Enterprise | Enterprise Level | Interactive | Multiple Dimensional Topologies | Enterprise Model |
| 3 | Domain | Domain Level | Groupware | Worldwide Network | Domain Model |
| 2 | Functional | Program Level | Desktop Automation | Local Networks | Program Model |
| 1 | Connected | Local/Site Level | Standard System Drivers | Simple Connection | Local |
| 0 | Isolated | Access Control | N/A | Independent | Private |

### 2.2 How is Interoperability Currently Achieved?

A systematic examination of programs for achieving interoperability reveals a number of required activities. In four of these activities agreement must be negotiated among the participants involved:

- Communications and Automated Data Processing (ADP) technical interface standards. These standards exist at the physical and data layers of the problem (e.g., interfaces among the data systems, modem, transmitter/receiver) to ensure that the systems are mutually compatible (i.e., signals can be automatically exchanged between them). This includes agreement on waveforms and modulation techniques.
- Message standards. There are three major aspects of message standards:
  - data elements: the types of information to be transmitted
  - data items: the allowable values of that information
  - message format: the order in which the data are arranged

  The process of negotiating these decisions is typically arduous and time consuming. This is because reconciliation involves resolving conflicting service procedures, doctrines, terminology, roles, and missions. In addition, these agreements frequently affect large inventories of legacy equipment and reach-back or reach-forward modifications can be quite costly.
- Database and applications standards. There are many variables that must be negotiated to ensure that information exchanged can be correctly stored and interpreted. This can be something as simple as the date. A US operator could well format the Fourth of July 2004

as 07-04-04 while his German counterpart would represent it 04-07-04. Ambiguities can ensue if agreement is not achieved on representing even the most basic variables.

- Operating procedures. The operating procedures associated with the use of multiple systems refer to those procedures to be followed by data system operators (e.g., interface procedures for the establishment of data links and exchange of tactical data). Those procedures should not be confused with the broader set of operational procedures that guide tactical actions.

In addition to negotiating actions for these factors, interoperability is achievable if the resulting configurations are thoroughly tested and certified, operators are well-trained to operate in interoperable modes, and strict configuration management controls are imposed on interfaces between evolving systems.

To consider how these steps can be implemented, consider two historical interoperability initiatives: Tactical Air Control Systems/Tactical Air Defense Systems (TACS/TADS) and the Army's Task Force XXI Advanced Warfighting Experiment (AWE).

### 2.2.1 TACS/TADS

During the 1970's, the TACS/TADS program was conducted under the aegis of the Joint Staff to ensure that key service systems that contributed to and used the air picture were able to exchange air track data accurately and unambiguously. These systems included, *inter alia,* the Army's TSQ-73 Missile Minder, the Navy's E-2C and Naval Tactical Data Systems (NTDS), and the Air Force's TSQ-91 Control and Reporting Center. To achieve that objective, a testbed was established in Southern California that stimulated the linked systems with live and/or simulated air data. This testbed enabled the participants to explore alternative operating procedures and standards for messages, databases, and applications in a controlled, structured fashion. The program concluded in the late 1970's with a live exercise, Solid Shield, which demonstrated the interoperability achieved among the systems. Note that it took approximately eight years to go from architectural vision to configuration management.

### 2.2.2 Task Force XXI AWE

During 1996 through 1997 timeframe, the Army conducted its Task Force XXI AWE (Reference 6). In 1995, as they prepared for the AWE, the Army began to realize that they had a serious interoperability problem. Even though the $C^4I$ components that supported the Fourth Infantry Division (4ID) were supposed to be interoperable (primarily the subordinate systems of the Army Tactical Command and Control System (ATCCS)), it soon became apparent that there were serious shortfalls. To ameliorate this problem, a Central Technical Simulation Facility (CTSF) was established at Fort Hood, TX. Using this facility, an iterative process was implemented whereby the subordinate system developers were assembled to redress technical problems, operational planners were called upon to evolve new operation concepts, trainers were tasked to train the operational users, and the operational users were asked to provide feedback on residual issues. Successive cycles of this process were implemented until interoperability had improved to the point where the AWE could be conducted successfully. Note that this process addressed each level of the physical, information, cognitive, and social domains of interoperability.

## 2.3 Why Is It Difficult to Achieve Interoperability of Information Technology Systems?

There are a host of reasons why it has proven difficult to implement interoperability successfully in prior programs. Fundamental to those problems is the balance between benefits and liabilities associated with these activities.

From a cost perspective, designing for interoperability implies a willingness to accept a complex set of liabilities and benefits. Indeed, currently there are strong disincentives for a program manager (PM) to pursue interoperability aggressively. Typically, PMs are acutely sensitive to five major liabilities that can be incurred:

- increased acquisition costs associated with the addition of common interoperable modes;
- added complexity and cost of adding features to achieve backward compatibility;
- increased time to acquire a system (i.e., time to agree on interoperability features and to perform the additional testing required to certify interoperability);
- increased complexity and cost associated with configuration management of the interfaces;
- increased size, weight, and power to accommodate modes that provide backward compatibility.

Conversely, the judicious application of interoperability could promote significant cost avoidances and reductions. Appropriate implementation of interoperability could promote broad savings in manpower and training. For example, if automated interfaces preclude the need for either liaison or "swivel chair" interoperability teams and their associated equipment, it could reduce substantially the life cycle costs of the fielded system. However, program managers generally have little incentive to consider this facet of costs in their cost-benefit tradeoffs.

Interoperability programs also give rise to a complex set of potential liabilities and benefits, from an operational perspective. There are several operational risks that must be carefully guarded against. With enhanced interoperability comes the attendant risk of new system vulnerabilities (e.g., the proliferation of viruses or "worms" that can infect a system). In addition, enhanced interoperability can introduce increased levels of information that could conceivably overload a system or even introduce extraneous or conflicting information.

Nevertheless, several major operational benefits can accrue if interoperability is implemented properly. First, automated interoperability can minimize delays when conveying information and minimize the likelihood of errors introduced through human intervention. These factors can be critical in mission areas, such as air defense, where mission effectiveness is sensitive to relatively short time delays and errors in target identification. Second, interoperability allows a common perception of the operational situation to be disseminated to a key set of decision makers. This proved to be of extreme value in the management of operations during Operation Iraqi Freedom in the Persian Gulf. In addition, the aviation forces of the US Air Force, Navy, and Marine Corps were able to pass air tasking order (ATO) information from one to the other electronically. This capability allowed aviation forces to co-ordinate strikes without the many hours of delay required to pass ATO information via hard copy (or floppy disk) as was necessary in Operation Desert Storm (Reference 7). Finally, if interoperability is implemented properly, it provides the potential for enhanced resistance to possible enemy actions (e.g., the ability to reconfigure networks if key nodes are destroyed or to reroute traffic to compensate for enemy efforts to jam key links) and can potentially provide additional flexibility and adaptability into the system (e.g., enabling the ad hoc interconnection of selected systems as might be required for changing conditions).

These observations suggest that the level of interoperability sought should be derived from a careful assessment of potential benefits and liabilities that are based on a broad and deep understanding of mission needs and program constraints. Once this conceptual balance has been struck, barriers remain that have historically impeded the successful implementation of interoperability. These historical barriers can be aggregated into five major categories:

institutional, program management, architectural and standards, operations, and systems. Each of these areas is discussed below.

### 2.3.1 Institutional

Until recently, no single organization has had responsibility for interoperability of IT systems. IT interoperability issues are frequently discussed in the Military Communications Electronics Board (MCEB) and intelligence interoperability issues are frequently discussed in the Military Intelligence Board (MIB). Although there are individuals who sit on both boards, there is no clear forum to address interoperability issues that involve $C^4$ and intelligence systems. The problem is far more difficult when the issues transcend national or interagency lines. Within the vacuum that exists, many "stovepipe" organizations have arisen to address localized interoperability issues. However, there have not been adequate institutional mechanisms to resolve interoperability problems that cut across those stovepipes.

A far-reaching Department of Defense (DOD) Inspector General's report of October 17, 2002 concluded that (Reference 8):

> Without consistent guidance that makes combat and materiel developers analyze programs using an operational architecture view, the DOD is at risk of developing systems that operate independently of other systems and of not fully realizing the benefits of interoperable DOD systems to satisfy the needs of the warfighter as outlined in Joint Vision 2020.

In commenting on the IG report, Lt. Gen. John Abizaid, then Director of the Joint Staff, said, "There is no joint process responsible and accountable for developing and acquiring joint command and control systems and integrating capabilities." (Reference 8). As discussed below, several institutional initiatives (e.g., CJCSI 3170, MID 912) have been undertaken to address this issue.

### 2.3.2 Program Management

Ultimately, much of the management responsibility for interoperability rests on the shoulders of the PM for a given system. However, the PM responds to incentives that tend to be relatively narrowly focused: the PM emphasizes the development of a system that provides specified performance within cost and schedule constraints. There are few incentives and therefore less attention paid to achieve (and maintain) interoperability. Thus, historically, little effort has been made to design interoperability into a program at its inception and, when programmatic adjustments are mandated (due to resource constraints or technical problems), little attempt has been made to coordinate cross-program adjustments to minimize fielding mismatches or cusps (i.e., instances when two non-interoperable systems are fielded; one newly deployed and the other being phased out). A positive development is that in the new DOD 5000-series acquisition documents, which guide acquisition procedures, interoperability is included as a key performance parameter, which raises its visibility (Reference 9).

### 2.3.3 Architectures and Standards

$C^4I$ systems are characterized by external interfaces that are complex, frequently changing, difficult to predict, and operational at multiple organizational levels (some inter-service, some multinational, some interagency). To achieve and maintain interoperability, it is vital that a sufficiently broad and detailed architectural vision be established that clearly articulates the objective relationship among systems and the proposed transition plan. Although there are some notable successes where this architectural vision has been created and adhered to, it is far more typical that an adequate architecture will not be developed, or if developed, not

updated in a timely way or adhered to. Here too the new 5000-series documents mandate that new systems be able to operate within a joint integrated architecture, subsuming operational, systems, and technical views (Reference 10).

It is becoming more widely recognized that the timely development and implementation of standards for $C^4I$ systems are a necessary (but not sufficient) condition for interoperability. At the same time, a profusion of organizations are involved in developing these standards. Although there are many apparent interrelationships among $C^4I$ standards activities, efforts to develop consistent policy for guiding their activities or reconciling conflicts have fallen short. In addition, the standards development process is frequently long and arduous, and sufficiently ambiguous so that "building to a standard" does not guarantee interoperability. It is not yet clear whether expanded procurement of commercial IT systems will alleviate this problem or not. Commercial systems bring their own set of interoperability problems, in particular their relatively short shelf life as compared to military systems (e.g., 18 months vice many years) and the reluctance of commercial IT providers to guarantee reach back interoperability with legacy systems (even their own) for the duration of use by the military.

### 2.3.4 Operations

Operationally, barriers to interoperability emerge due to the unique demands posed by specific theaters of operation and operations with heterogeneous partners. In many instances, a Combatant Commander is provided with $C^4I$ systems that can operate across Service lines but cannot operate with other agency or multinational $C^4I$ systems. This is a continuing problem that is exacerbated by differences among interagency and multinational partners in language, doctrine, security policies, and concepts of operation. In addition, many Combatant Commanders lack the assets needed to implement configuration management to ensure that interoperability is maintained as systems evolve or new systems are fielded.

### 2.3.5 Systems

There are many barriers at the system level that impede the successful attainment of interoperability. These include system inventory, service-unique needs, security, testing, and certification. For many of the $C^4I$ systems of interest, large numbers of equipment exist in the inventory that are expected to be operational well into the twenty-first century. For example, there are many thousand high frequency (HF) radios in each service employing different waveforms and crypto-gear. If new HF radios are to be interoperable with this inventory, it will place an extreme burden on these new radios to have many backward-compatible interoperable modes. As an example, the Joint Tactical Radio System (JTRS) is addressing this issue by creating a software configurable radio that will emulate selected legacy systems. However, the different clusters of JTRS will still be limited in the types of waveforms that they can emulate.

The Services' needs for $C^4I$ systems emerge from their unique roles, missions, and concepts of operation. Since these unique factors are paramount in their minds as they develop a new system, extreme attention must be paid to the problem of interoperability to ensure that some interoperable modes are developed where needed. A classic example of this problem arose in the case of the Joint Tactical Information Distribution System (JTIDS). Continuous dialogue between the Air Force and Navy occurred over a fifteen-year period (stimulated by the Office of the Secretary of Defense) to ensure that waveforms and access modes were selected that enabled some level of interoperability. Although the issue was later rendered moot when the Navy elected to procure the USAF system, this incident reveals the difficulties associated with reconciling the competing demands of interoperability and service-unique requirements.

Advances in security are, paradoxically, creating serious interoperability problems. As an illustration, in several areas it is not permissible to provide the latest crypto-gear to US allies (e.g., the Secure Telephone Unit (STU) program), yet many new systems lack backward compatible modes.

Recent experiences with interoperability programs have highlighted the value of testbeds as a means of identifying and stimulating the resolution of interoperability problems. As examples, the two testbeds cited above (i.e., the TACS/TADS testbed in Southern California and the CTSF at Ft. Hood, TX) were instrumental in supporting prior successful interoperability initiatives.

### 2.4 How Are We Doing in Achieving Interoperability?

Due to the complexity of the interoperability landscape, it is very difficult to answer the question of how well we are doing in achieving appropriate levels of interoperability. However, the results of the recent military operations in Kosovo, Afghanistan, and Iraq provide a partial answer. As documented in a recent GAO study, "Improvements in force networks and in the use of precision weapons are clearly primary reasons for the overwhelming combat power demonstrated in recent operations" (Reference 11). The report goes on to conclude: "Not withstanding these improvements, certain barriers inhibit continued progress in implementing the new strategy." One of the key barriers that the report cited was "A lack of standardized, interoperable systems and equipment, which reduces effectiveness by requiring operations to be slowed to manually reconcile information from multiple systems and limiting access to needed capabilities among military systems."

Thus, although DOD appears to be making headway in redressing key interoperability shortfalls, it is clear that major deficiencies still persist.

### 2.5 Key Trends Affecting Interoperability

Although a review of prior events can tell us a great deal about the interoperability issue, interoperability is a dynamic problem. Consequently, it is important to discern trends that will affect interoperability in both negative and positive ways. In the following, we discuss briefly the results of such a trend analysis, which explores key activities and events ranging from "requirements pull" (e.g., geopolitical trends, emerging strategic vision) to "technology push" (e.g., new opportunities offered by technological advancements). Selected initiatives that have the potential to ameliorate interoperability issues are described and discussed in detail.

#### 2.5.1 Geopolitical Trends

Historically, military organizations have organized, equipped, and trained the bulk of their forces to respond to major theater wars. However, in recent years military operations have been characterized by demanding expeditionary operations followed immediately by stabilization and reconstruction (S&R) operations involving a variety of JIM+ partners. Operation Iraqi Freedom and Operation Enduring Freedom (in Afghanistan) follow this pattern. In addition, US and allied forces are, at any one time, engaged in one or more humanitarian relief efforts or non-combatant evacuation operations (NEO), peacekeeping and peacemaking (e.g., Operation Joint Endeavor in the Former Yugoslavia). In each instance, these operations revealed significant interoperability shortfalls among the participating forces and other participating parties (e.g., NGOs, such as the Red Cross). We expect the number and diversity of these operations to remain high throughout the decade, which puts additional stresses on the JIM+ interoperability problem.

#### 2.5.2 International Security Trends

Consistent with the geopolitical trends, it is notable that coalitions have become the rule in S&R operations. Up to now these coalitions have consisted primarily of members of NATO with whom the US has a long history of co-operation. These coalition members arrive with a shared set of doctrine, standards, and concepts of operation that support interoperability. However, the newest NATO nations have not yet gained this experience and, indeed, it has become increasingly frequent that additional regional nations and NGOs participate in these operations on an ad hoc basis bringing with them heterogeneous languages, equipment, and training. Experience has demonstrated that it is extremely challenging to achieve even the most rudimentary interoperability with those entities.

One encouraging interoperability trend that may ameliorate a segment of this problem is DOT&E's Joint Methodology to Assess C4ISR Architectures (JMACA) (Reference 12). Currently the Joint Task Force (JTF) commander lacks the means to identify JIM+ interoperability deficiencies and solutions rapidly. This Joint T&E activity is developing and validating a set of C4ISR architecture assessment tools that should mitigate selected aspects of the problem.

### 2.5.3 Strategic Vision

Within the US, considerable focus has been placed on the transformation of its armed forces, driven in large part by the ongoing revolution in information technology. This view is accentuated by the observation that the existing military is a product of the Industrial Age while the transformed military will be a product of the Information Age (Reference 1). This information technology driven transformation is highlighted in a series of studies issued by the Office of Force Transformation (Reference 13) and by the Chairman, JCS in his Joint Vision 2020. The Joint Vision 2020 envisions forces characterized by extensive use of precision force, enhanced battlespace awareness, and advanced $C^4I$. The implication of this vision on interoperability is as follows: by increasing the visibility of the interoperability problem a major burden is placed on the community to achieve significantly more complex and challenging levels of JIM+ interoperability.

Furthermore, in the wake of the terrorist attacks of September 11, 2001, the homeland security mission has become one of the United States' highest priorities. This mission requires extensive interoperability among DOD (e.g., USNORTHCOM), key federal agencies (e.g., Department of Homeland Security, Department of Justice), and regional, state, and local organizations (e.g., police, fire, and emergency medical personnel). It will take a substantial period of time to achieve these desired levels of interoperability.

### 2.5.4 Institutional Initiatives

There are a number of institutional initiatives that are influencing the interoperability problem. These include new DOD policy and guidance, an increased leadership role for USJFCOM, an interest in the concept of "interdependency," and increased emphasis on the use of commercial-off-the-shelf (COTS) products in DOD.

#### 2.5.4.1 Policy and Guidance

Several key interoperability-related policy and guidance documents have been issued over the past several years. These include the following:

- CJCSI 3170 establishing a Joint Capabilities Integration and Development System (JCIDS) to supersede the earlier requirements system and to ensure that key new systems are "born joint" (Reference 14).
- DOD Series 5000 modifying the acquisition process so that evolutionary acquisition strategies are the preferred approach to satisfying operational needs vice the "grand

design, waterfall" model. It specifies that interoperability must be addressed to conduct joint and combined operations successfully, emphasizing relevant families-of-systems (Reference 9).

- CJCSI 6212 entitled "Interoperability and Supportability of National Security Systems and Information Technology Systems" (Reference 15). This instruction directs the Joint Staff to certify interoperability key performance parameters, Information Exchange Requirements, and C4I Support Plans, and approve Joint Interoperability Test Command (JITC) interoperability certification.
- DOD Directive 8100.1 entitled Global Information Grid (GIG) Overarching Policy (Reference 16). The GIG is a vision for a "globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel." It is intended to provide interfaces to coalition, allied, and non-DOD users and systems. If this vision (and associated architecture, standards, and principles) can be implemented successfully it should contribute substantially to enhanced long term JIM+ interoperability.
- DOD Directive 4630.5 entitled "Interoperability and Supportability of Information Technology and National Security Systems" (Reference 17). As a key facet of this directive, it establishes the Net-Ready Key Performance Parameter.

Furthermore, in May 2003, ASD(NII) issued the DoD Net-Centric Data Strategy (Reference 18). That strategy seeks to support data interoperability through the following goal: "Many-to-many exchanges of data occur between systems through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed." In order to achieve that goal, the strategy recommends the following approach: register metadata, associate format-related metadata, identify key interfaces between systems, and comply with Net-Centric interface standards.

#### 2.5.4.2 USJFCOM Role

Management Initiative Decision (MID) 912 assigned USJFCOM the responsibility for Joint Battle Management C2 (JBMC2) to lead operational to tactical interoperability initiatives and to address Combatant Commanders' needs in the area (Reference 19). Consistent with that assignment, USJFCOM is refining a JBMC2 Road Map with four strategic elements: warfighter-driven concept developments; plans to make interoperable or converge JBMC2 programs; several JBMC2 initiatives focusing on the development of a family of interoperable pictures; and joint interoperability test plans (Reference 20). Within USJFCOM, the Joint Interoperability and Integration (JI&I) Office in J8 has a central role in discharging that responsibility and is developing an Interoperability Technology Demonstration Center (ITDC) (Reference 21). Furthermore, several other organizations in USJFCOM are developing key testbeds and playing significant roles in interoperability through their responsibilities in education and training (J7) and prototyping (J9).

#### 2.5.4.3 Interdependency

The joint community has begun to go beyond the continuum of "integrated-interoperable-compatible" (described in section 2.1.2). In selected mission areas they seek to achieve "interdependency" among the services. For example, there are discussions underway in which a "contract" would be forged between the Air Force and Army in which the Army would eliminate some of its artillery resources and rely more extensively on timely, precise indirect fire support from the Air Force. The Joint Staff has characterized this interdependency as follows: "It refers

to a mode of operations based upon a high degree of mutual trust where members contribute to common ends synergistically and rely on each other for certain essential capabilities rather than duplicating them organically." This level of shared dependency will have very stringent interoperability implications.

#### 2.5.4.4 COTS Products

In response to guidance from then-Secretary of Defense William Perry military organizations are making increasing use of commercial standards and practices in the acquisition of new systems (Reference 22). Although the intent is to harness the vitality of the information industry and realize significant savings in cost, its impact on the interoperability problem is uncertain. Positive effects include the military's employment of accepted community-wide standards. However, commercial products evolve over rapid cycle times (e.g., on the order of six to eighteen months for some software packages), and this in itself poses interoperability problems. For example, many enhanced packages have only limited backward compatibility. Systems composed of mixes of commercial packages may cease to be interoperable as new versions are released. Furthermore, many commercial products are inadequately tested or documented.

### 2.5.5 GIG and Enterprise Service Trends

One of the most important DOD initiatives, from the perspective of interoperability, is the GIG and its related enterprise services. As observed in a recent GAO report, "The GIG is a huge and complex undertaking that is intended to integrate virtually all of DOD information systems, services, and applications into one seamless, reliable, and secure network" (Reference 23). However, the GAO went on to note that "The most critical challenge ahead for the DOD is making the GIG a reality." At this preliminary stage, it is not feasible to predict accurately how successful the DOD will be in this undertaking. However, in an assessment of the GIG's challenges and risks, the GAO has cautioned that "…many of which have not been successfully overcome in smaller-scale efforts and many of which require significant changes in DOD's culture."

As an adjunct to the GIG initiative, DOD is also seeking to deploy trusted enterprise services. As one element, Net-Centric Enterprise Services (NCES) are being developed to provide information and data services to all GIG users (Reference 24). There are a total of nine Core Enterprise Services (i.e., Application, Mediation, User Assistance, Messaging, Enterprise Systems Management, Information Assurance/Security, Discovery, Storage, and Collaboration) that are scheduled to evolve in three spirals by FY10. Furthermore, DOD is seeking to enhance sensemaking through the development of a Horizontal Fusion portfolio (Reference 25). The objective of this latter initiative is to develop and provide net-centric means/tools to enable the smart pull and fusion of data by users through inter-related capability improvements. DOD is demonstrating the capabilities of this evolving portfolio through Quantum Leap, an annual event.

These initiatives have the potential to transform the very nature of the interoperability problem. However, there are profound issues on resources, governance, management, and culture that must be resolved if these initiatives are to achieve their stated goals.

### 2.5.6 System Trends

There are a number of trends in the systems arena that will have a mixed impact on interoperability. First, there is a great deal of interest among commercial manufacturers of software to exploit object-oriented technology. One important development is the introduction and refinement of the concept of an Object Request Broker (ORB). One manifestation of this technology is the Common Object Request Broker Architecture (CORBA), which has been created to facilitate communication between distributed objects in an environment made up of

different types of hardware and software components (Reference 26). This "middleware" technology may ameliorate many of the interoperability problems associated with heterogeneous mixes of systems. However, to date, no standards have been universally adapted by the major producers of commercial software. In addition, commercial information systems are changing so quickly that rapid obsolescence is becoming commonplace. This implies that it will be even more difficult to maintain interoperability among fielded systems (i.e., systems that fail to modernize may cease to be interoperable with those systems that elect to update embedded packages that are evolving rapidly).

### 2.5.7 Data Model Trends

The objective of the Command and Control Information Exchange Data Model (C2IEDM) is to define the minimum operational and technical requirements to be included within system specifications that will allow national C2 systems to interoperate by the automatic exchange of data (Reference 27). The data specification focuses on information necessary to understand the basic operation picture in an area of interest and the depiction of planned and actual activity. The development of the model is being performed by a Multilateral Interoperability Programme (MIP), comprised of ten full members from the NATO community and sixteen associate members. The MIP is currently developing an upgraded reference model, denoted as the JC3IEDM, which is planned for release toward the end of CY2005.

### 2.5.8 Technology Trends

We are witnessing a number of technology trends that may ameliorate several historical barriers to interoperability. At the network layer, efforts to make “N” unique systems interoperable required N(N-1)/2 actions. Thus if ten systems were to be made interoperable, it required forty-five separate interoperability activities. Conversely, with DOD promulgation of a “Net Ready” Key Performance Parameter and migration to Internet Protocol (IP)-based interoperability, each future system will have to deal with a single interface to the network. Hence, if ten web-based systems are to be made interoperable, it requires ten interoperability activities (i.e., a linear vice an exponential level of effort). Furthermore, at the data layer the defense community is aggressively pursuing Extensible Markup Language (XML) to index the content of the messages that they are exchanging. If the defense community can agree on XML standards and implement them widely, it will greatly enhance the automated exchange of information (Reference 28).

In addition, at the application layer, significant advances are being made in speech understanding, message understanding, intelligent storage and retrieval, decision support systems, intelligent agents, and enhanced network management. As these technologies mature, they have the potential to ameliorate many of the problems that currently limit interoperability (e.g., compensating for differences in the languages spoken by participating forces).

In September 2004, the Network Centric Operations Industry Consortium (NCOIC) was announced, drawing on twenty-eight major defense firms (e.g., Boeing, Lockheed Martin, Northrop Grumman) and commercial IT firms (e.g., Microsoft, Oracle) (Reference 29). The mission of the Consortium is “to help accelerate the achievement of increased levels of interoperability in a network centric environment within, and amongst, all levels of the government of the US and its allies involved in JIM operations.” The four primary tenets of the consortium vision include developing a Network Centric Environment, providing assured interoperability, embracing open standards, and establishing common principles and processes. The proposed deliverables from the Consortium include the development of customer requirements (e.g., evaluate architectures related to programs such as the GIG), the development

and refinement of an NCO Reference Model (e.g., identify open standards and their patterns of use; help develop standards where none exist), and the establishment of an education outreach program. Given the experience and skills of the Consortium membership, this must be viewed as a serious initiative that has the potential to make a substantive contribution to several technical interoperability issues.

### 2.5.9 Testbed Trends

There is increased appreciation of the value of testbeds to showcase new interoperability technologies and to demonstrate alternative interoperability concepts. Moreover, even those designed and operated by individual services increasingly accommodate testing for interoperability with other service systems. For example, the Army's CTSF at Ft. Hood, TX, is being employed to explore future joint Blue Force Tracking options and fratricide reduction demonstrations.

There are three evolving testbeds that have the potential to play major roles in ameliorating interoperability problems. These testbeds are focused on joint training, near-term (e.g., 12 month) acquisitions, and longer-term acquisitions of interoperable systems.

- Training. Under the aegis of USJFCOM, a Joint National Training Capability (JNTC) is emerging (Reference 30). The goal of this initiative is to create a simulated environment by 2009 that will have the capability to support JIM audiences. The persistent network will address joint training, experimentation, testing, education, and mission rehearsal, by linking $C^2$, training facilities, ranges, and simulation centers throughout the world. However, the complexity and size of the operation will limit its use to a handful of iterations per year.
- Near-Term Acquisitions. The Coalition Warrior Interoperability Demonstration (CWID) (formerly known as the Joint Warrior Interoperability Demonstration (JWID)) is a yearly event that draws on service, agency, and multinational participants to identify short-term solutions (i.e.., 6 – 12 months) for enhancing JIM interoperability (Reference 31)/ CWID is conducted in a simulated, world-wide operational environment to provide an appropriate context for validation of proposed interoperable $C^4ISR$ solutions. USNORTHCOM was designated as the host command for 2004 and 2005, thereby expanding the participants to include a broad array of homeland security actors. Called the "Olympics of Interoperability" by Lt. Gen Harry D. Raduege Jr, Director of DISA, it could play an important niche role in addressing short term interoperability issues.
- Longer Term Acquisitions. The Joint Distributed Engineering Plant (JDEP) program is emerging as a DOD-wide effort to improve interoperability by providing the infrastructure needed to support integration testing and evaluation in a replicated battlefield environment (Reference 32). Physically, JDEP will employ the High Level Architecture (HLA) to connect combat systems sites, emulate tactical data links, and synchronize sensor stimulation. Functionally, it will replicate joint force combat systems and $C^4I$, provide a controlled, repeatable environment, and support the assessment of system-of-systems interoperability and effectiveness. Although this initiative is promising, there are challenges in funding and its scope does not embrace the full JIM+ problem.

## 3. Key Residual Challenges

Although initiatives cited above will serve to ameliorate some of the existing and emerging interoperability issues, there are many challenges that remain to be confronted from

the perspective of institutions, program management, architectures and standards, operations, and systems.

### 3.1 Institutional Challenges

Although several initiatives have been launched to break down cultural "stovepipes", these stovepipes are deep and pervasive. They can be seen within JIM+ communities since they are rooted in profound cultural differences. These barriers will not disappear rapidly. This point was emphasized recently by ADM Edmund Giambastiani, commander of USJFCOM, who stated that "the iron middle" (e.g., middle managers on the military side) have cultural blinders that stimulate them to do "what is best for the individual mid-level officer and that officer's individual program, but it's bad for jointness" (Reference 33).

### 3.2 Program Management Challenges

The increased interest in acquiring a system-of-systems provides enhanced opportunities to create and sustain interoperable solutions (e.g., the Army's Future Combat Systems (FCS)). However, these "system-of-systems" are inevitably dependent on a broad array of JIM+ systems to accomplish their mission and most of those systems are beyond the program management control of the "system-of-systems" PM. For example, the FCS is strongly dependent on the JTRS, which is beyond the control of the FCS PM.

Furthermore, as Evolutionary Acquisition and Spiral Development become the norm in systems acquisition, systems will evolve in increments on a time scale consistent with the issuance of updated versions of commercial products (e.g., on the order of 18 months). It will be a major challenge to maintain interoperability within and across system lines in the face of these continual changes.

### 3.3 Architectural and Standards Challenges

It is widely recognized that the creation and adherence to architectures and widely accepted standards are important facets of interoperability. However, the standards process is extremely slow and laborious and the pace of technological innovation in information systems is frequently outstripping it. It remains to be seen whether a meaningful standards process can be implemented without its being a barrier to interoperability. In addition, although the potential value of overarching architectures is widely recognized, it is still unclear how one can generate architectural products of sufficient breadth and detail and keep them current. This is of particular concern for the GIG given its enormous scope.

### 3.4 Operational Challenges

A fundamental, residual challenge to interoperability is coping with the multitude of differences among interagency and multinational partners. This includes, but is not limited to, differences in equipment, language, doctrine, concepts of operation, and training. There are meaningful steps that can be taken to attack these barriers (e.g., cooperative development and procurement of systems; extensive language training and the development of new technology to facilitate language understanding; cross-education of personnel at defense colleges; and extensive JIM+ exercises). However, it must be recognized that many of these obstacles are so challenging that they will limit the levels of JIM+ interoperability that are achievable in the foreseeable future. In addition, steps need to be taken in the short-term that would help the combatant commands to better manage in-theater $C^4I$ assets (e.g., assemble ad hoc interoperable systems-of-systems to prepare for an imminent operation, and responsively inject innovative information technology into systems to redress key shortfalls).

### 3.5 System Challenges

One of the fundamental barriers to JIM+ interoperability is the issue of releasibility of security systems and devices outside of DOD. Consideration should be given to developing future security systems that are either releasable to non-DOD participants or which possess modes that are interoperable with their systems. In addition, it should be recognized that thorough testing is a critical element of the interoperability challenge. Although important steps are being taken to address this issue (e.g., CJCSI 6212), we currently lack the resources needed to respond to the full JIM+ testing challenge.

## 4. Summary

Interoperability has been, and will continue to be, an exceptionally challenging problem. The DoD is pressing on with transformation of US forces whose foundation is dominant battlespace knowledge and the ability to share large volumes of information promptly and reliably. This puts a high premium on interoperability among IT systems across JIM+ boundaries. Initiatives have been launched to enhance management oversight, to provide architectural vision, to highlight major interoperability shortfalls, to test and experiment with IT systems, and to showcase enhancements in interoperability. However, the magnitude of the problem is such that major challenges persist. These challenges are particularly daunting because many of them are cultural in nature. They involve such difficult tasks as breaking down community "stovepipes," coping with differences in language and concepts of operations, and changing the program management culture. These observations reinforce the point that interoperability is not a bounded problem that can be "solved," but a continually evolving problem that must be attended to on an ongoing basis.

## 5. References


1. David S. Alberts and Richard E. Hayes (with an Introduction by John Stenbit), *Power to the Edge*, Command and Control Research Program, ISBN 1-893723-13-5, June 2003.
2. *Joint Vision 2020*, Joint Chiefs of Staff (US Government Printing Office, Washington DC, June 2000). Available at http://www.dtic.mil/jointvision/jvpub2.htm.
3. Robert Nutwell and Paul Szabados, *Joint Information Interoperability: data-sharing deficiencies among the services require top-level attention,* Armed Forces Journal International, June 2002.
4. C4ISR Architecture Working Group, *Levels of Information Systems Interoperability (LISI),* 30 March 1998 (posted at www.defenselink.mil/nii/org/cio/i3/lisirpt.pdf).
5. Mark Kasunic and William Anderson, *Measuring Systems Interoperability: Challenges and Opportunities*, SEI, CMU/SEI-2004-TN-003, April 2004.
6. Annette J. Krygiel, *Behind the Wizard's Curtain*, Command and Control Research Program, ISBN 1-57906-018-8, July 1999.
7. Stuart H. Starr, *C3I for Coalition Warfare: Lessons Learned from Desert Shield/Desert Storm*, Proceedings of Symposium on Future of Security Role of the UN, pp 30 – 35, NDU, Fort McNair, 9-10 October 1991.
8. *Implementation of Interoperability and Information Assurance Policies for Acquisition of DOD Weapon Systems*, Department of Defense Office of the Inspector General Report No. D-2003-011, Project No. D2002AE-0009.000 (October 17, 2002). Available at http://www.dodig.osd.mil/audit/reports/fy03/03-011.pdf.
9. Department of Defense Directives 5000.1 and 5000.2, May 12, 2003 (accessible at http://hfetag.dtic.mil/dod5000.html).

10. DOD Architectural Framework (DODAF) Version 1.0, Feb 9, 2004 (accessible at http://www.defenselink.mil/nii).
11. *Military Operations: Recent Campaigns Benefited from Improved Communications and Technology, but Barriers to Continued Progress Remain*, GAO, June 2004.
12. Len Zimmermann, *Joint Methodology to Assess C4ISR Architectures (JMACA),* Joint Test & Evaluation, brief to JFCOM J8, 12 March 2004 (accessible at http://www.jmaca.jte.osd.mil/Documents/JFCOMJ8JMACAbrief.ppt).
13. See for example documents posted at http://www.oft.osd.mil/library/library.cfm?libcol=6.
14. CJCSI 3170.01D, *Joint Capabilities Integration & Development System,* 12 March 2004 (accessible at http://www.teao.saic.com/jfcom/ier/documents/3170_01D_12_Mar_04.pdf).
15. CJCSI 6212.01C, *Interoperability and Supportability of Information Technology and National Security Systems,* 20 Nov 2003.
16. DODD 1800.1, *GIG Overarching Policy,* September 19, 2002 (accessible at www.dtic.mil/whs/directives/corres/pdf2/81001p.pdf).
17. DODD 4630.5, *Interoperability and Supportability of Information Technology and National Security Systems,* January 11, 2002.
18. John Stenbit, *DoD Net-Centric Data Strategy,* May 9, 2003.
19. *Information and Command and Control,* Aerospace America, AIAA, December 2003.
20. *JBMC2 Roadmap Development,* Rand NDRI, March 2004 (accessible at www.dtic.mil/ndia/2004interop/Wed/jbmc2rand.ppt).
21. Michael Wimbish, *New Center to help foster interoperability,* USJFCOM, April 28, 2003 (accessible at http://www.jfcom.mil/newslink/storyarchive/2003/pa042803.htm).
22. Secretary of Defense William Perry, memorandum on use of COTS, 29 June 1994.
23. *Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation,* GAO, July 2004.
24. *Net Centric Enterprise Services (NCES)* (accessible at www.disa.mil/main/nces.html).
25. *Horizontal Fusion/Quantum Leap* (www.horizontalfusion.dtic.mil).
26. *Object Request Broker/Common Object Request Broker Architecture* (accessible at http://www.omg.org/gettingstarted/corbafaq.htm).
27. Gene Simaitis, *An Introduction to C2 Information Exchange Data Model (C2IEDM),* Institute for Defense Analyses, 8 November 2004.
28. NCOIC Home page (http://www.ncoic.org/index.htm).
29. Robert W. Miller, Mary Ann Malloy, Ed Masek, *Formatted Message Modernization Exploits XML Technologies,* The Edge, Summer 2004, Volume 8, Number 1 (www.mitre.org/edge).
30. *Joint National Training Capability* (accessible at http://www.jfcom.mil/about/fact=jntc.htm).
31. *CWID* (accessible at http://www.cwid.js.mil/c/extranet/home).
32. *Joint Distributed Engineering Plant (JDEP)* (accessible at http://in.disa.mil/jdep.html).
33. *Adm. Giambastiani Slams Defense Industry, Mid-Level Procurement Officers,* Defense Today, page 1, August 5, 2004.