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

> Dr. Stuart H. Starr BRI and CTNSP, NDU 15 June 2005

Agenda

- Nature of the Problem
- Key Trends and Their Implications
- Residual Interoperability Challenges
- Summary

What is Interoperability?

- Systems are interoperable if they have two key factors in common
 - They allow units to exchange data in a prescribed manner
 - They use the extracted information to operate together effectively
- Four complementary perspectives of the term include
 - Operational perspective
 - The "Integration Continuum"
 - Domains of warfare
 - Systems perspective

Operational Perspective

Level	Characterization
1	Totally non-interoperable (separate and independent systems)
2	Limited exchange of information via liaison teams
3	"Swivel chair" interoperability
4	Restricted, automated interoperability
5	Automated interoperability, consistent with operational needs

How is Interoperability Currently Achieved?



Representative Case Studies

- Selected case studies
 - Tactical Air Control System/Tactical Air Defense System (TACS/TADS) program
 - Task Force XXI Advanced Warfare Experiment (AWE)
- Key lessons learned
 - The need to iterate!
 - The value of a test bed
 - The time needed to achieve interoperability

Why is it Difficult to Achieve Interoperability -- Costs

- Liabilities (from a Program Manager perspective)
 - Increased costs associated with common interoperable modes
 - Added complexity and cost of adding features to achieve backward compatibility
 - Increased time to acquire a system
 - Increased complexity and cost for configuration management
 - Increased size, power, weight
- Benefits (macro-perspective)
 - Cost avoidances and reductions (e.g., manpower, training)

Why is it Difficult to Achieve Interoperability -- Operations

- Potential liabilities
 - New system vulnerabilities (e.g., viruses)
 - Data or information "overload"
- Potential benefits
 - Minimize delays, errors
 - Allow common perception of the operational situation to be shared
 - Enhance resistance to potential enemy actions

Why is it Difficult to Achieve Interoperability -- Operations

- Potential liabilities
 - New system vulnerabilities (e.g., viruses)
 - Data or information "overload"
- Potential benefits
 - Minimize delays, errors
 - Allow common perception of the operational situation to be shared
 - Enhance resistance to potential enemy actions

Ergo, a careful balance must be struck

Historical Barriers to Interoperability

- Institutional -- no single organization has had responsibility for interoperability
- Program management -- the PM responds to incentives that tend be relatively narrowly focused
- Architectures and standards -- external interfaces are complex, frequently changing, difficult to predict, and at multiple organizational levels
- Operations -- unique demands posed by specific AORs and operations with heterogeneous partners
- Systems -- inventory, Service-unique needs, security, testing, certification

How Are We Doing in Achieving Interoperability (GAO Perspective)?

- "Improvements in force networks and in the use of precision weapons are clearly primary reasons for the overwhelming combat power demonstrated in recent operations."
- "Not withstanding these improvements, certain barriers inhibit continued progress in implementing the new strategy."
- A key barrier is "... 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."

Agenda

- Nature of the Problem
- Key Trends and Their Implications
- Residual Interoperability Challenges
- Summary

Key Trends and Their Impact



Geopolitical Trends

• Trends

- Demanding expeditionary operations followed immediately by stabilization and reconstruction (S&R) operations (e.g., OEF, OIF)
- Coincident involvement in
 - Humanitarian assistance (HA)/Disaster Relief (DR)
 - Non-combatant evacuation operations (NEO)
 - Peacekeeping / Peacemaking (e.g., OJE)
- Implications: Need for Joint-Interagency-Multinational-"Plus" (JIM+) interoperability

Timeline of Recent US Policy Initiatives



Institutional Initiatives: GIG

• Trends

- "The GIG is a huge and complex undertaking that is intended to integrate virtually all of DoD information systems, service, and applications into one seamless, reliable, and secure network" (GAO)
- Implications --
 - There are major challenges and risks:
 - "... many of which have not been successfully overcome in smaller-scale efforts..."
 - "...many of which require significant changes in DoD's culture".

Institutional Initiatives: Industrial Association Initiatives

- Trends: A number of industrial associations have begun initiatives to mitigate barriers to enhanced interoperability and net-centricity
 - Network Centric Operations Industry Consortium (NCOIC) (September 2004)
 - Net Centric Operations Industry Forum (NCOIF) (February 2005)
 - World Wide Consortium for the Grid (W2COG)
- Implications: The roles and relationships of these initiatives should be clarified to ensure that they are complementary, not redundant

Technology Trends

- Trends
 - "Net ready" actions, transforming the N(N-1)/2 problem to the N problem
 - Aggressive use of Extensible Markup Language (XML)
- Implications
 - Promising approaches to address the interoperability problem

Testbed Trends

- Trends
 - Increased appreciation of the value of testbeds to
 - Showcase new interoperability technologies
 - Demonstrate alternative interoperability concepts
 - Evolving testbeds include, inter alia,
 - Joint National Training Capability (JNTC)
 - Coalition Warrior Interoperability Demonstration (CWID) / Combined Endeavor
 - Joint Distributed Engineering Plant (JDEP)
 - Defense industrial testbeds (e.g., Boeing, Lockheed Martin, Northrop Grumman)
- Implications
 - Promising tools are emerging to address significant interoperability issues

Agenda

- Nature of the Problem
- Key Trends and Their Implications
- Residual Interoperability Challenges
- Summary

Key Residual Challenges (1 of 2)

- Institutional Challenges
 - Convincing the "iron middle" (e.g., middle managers on the military side) to do what is best for jointness
- Program Management Challenges
 - Coping with systems that are outside of the PM control
- Architectural and Standards Challenges
 - Coping with the slow pace of the standards process
 - Using architectures to manage the process

Key Residual Challenges (2 of 2)

- Operational Challenges
 - Coping with all of the dimensions of JIM+ interoperability
 - Helping the Combatant Commands to better manage in-theater C4I assets
- Systems Challenges
 - Dealing with releasibility of security systems and devices outside of DoD
 - Performing adequate interoperability testing

Agenda

- Nature of the Problem
- Key Trends and Their Implications
- Residual Interoperability Challenges
- Summary

Summary

- Interoperability has been, and will continue to be, an exceptionally challenging problem
- Geopolitical trends (e.g., the need to work with *ad hoc* coalitions of the willing) and Transformation of the military (e.g., net centric operations) make the problem even more important
- However, it must be recognized that interoperability is not a bounded problem that can be "solved" but a complex set of issues that must be "managed"

Interoperability Problems Tend to be Complex, Poorly Defined



"Vacuums, black holes, antimatter, *Interoperability* -It's the elusive and intangible which appeals to me"

Back-up Material

"Integration Continuum"

- Integration -- going beyond interoperability to involve some degree of functional dependence
- Compatibility -- where systems do not interfere with each other's functions

Bottom line: Interoperable systems - Need not be integrated

- Are by necessity compatible

NCW Four Key Domains

Physical Domain

where strike, protect, and maneuver take place across different environments

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

Social Domain

where force entities interact

Systems Perspective: LISI Reference Model

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

How is Interoperability Currently Achieved?

- Agreement and achievement of seven activities must be accomplished to achieve interoperability
 - Communications and automated data processing technical interface standards
 - Message standards (re: data elements, data items, and message format)
 - Database and applications standards
 - Operating procedures
 - Testing and certification
 - Well-trained operators
 - Strict configuration management controls

Key Trends Affecting Interoperability

- Geopolitical trends
- International security trends
- Strategic vision
- Institutional initiatives
 - Policy and guidance
 - USJFCOM role
 - Interdependency
 - COTS products
 - GIG and Enterprise Service trends
- System trends
- Technology trends
- Testbed trends

International Security Trends

- Trends
 - Coalitions of the willing have become the rule
 - NGOs are playing an increasingly important role
 - Many participants
 - Lack a shared set of doctrine, standards, and concepts of operation
 - Have heterogeneous languages, equipment, training
- Implications
 - It is extremely challenging to achieve even the most rudimentary levels of interoperability
 - Joint Methodology to Assess C4ISR Architectures (JMACA) is developing C4ISR architectural tools that may mitigate selected aspects of the problem

Strategic Vision

- Trend
 - Transformation from an Industrial Age to an Information Age military
 - The Homeland Security mission has become one of the US' highest priorities
- Implications
 - Goal of achieving significantly more complex and challenging levels of JIM+ interoperability
 - Specifically, interest in enhancing interoperability among DoD, key federal agencies, regional, state, and local organizations

Institutional Initiatives: Policy & Guidance

- Trends -- new DoD policy and guidance; e.g.,
 - CJCSI 3170 (JCIDS), to ensure new systems are "born joint"
 - DoDD 5000, stressing evolutionary acquisition
 - CJCSI 6212, providing guidance on interoperability testing and certification
 - DoD 8100, providing policy on the GIG
 - DoDD 8110, establishing instructions on multinational information sharing
 - DoDD 8320.2, establishing a strategy for data sharing in a net-centric DoD
 - DoDD 4630, establishing the "net ready" KPP
 - Net-Centric Operations and Warfare Reference Model (NCOW RM), describing the transition to GIG Architecture Version 2
 - Net Centric Checklist, helping PMs understand the net-centric attributes their programs need to implement
- Implications -- renewed emphasis and guidance on interoperability

Institutional Initiatives: Interdependency

- Trends
 - Going beyond the continuum of "integratedinteroperable-compatible"
 - Interdependency "… refers to a mode of operation 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"
- Implications
 - Interdependency will have very stringent interoperability implications

Institutional Initiatives: USJFCOM Role

• Trend

- MID 912 assigned USJFCOM the responsibility for Joint Battle Management C2 (JBMC2) to
 - Lead operational to tactical interoperability initiatives
 - Address Combatant Commanders' needs in the area
- Implications
 - USJFCOM is playing a major leadership role in addressing interoperability issues
 - Several testbeds are emerging in JFCOM to support enhanced interoperability

Institutional Initiatives: Enterprise Services

- Trend:
 - Net Centric Enterprise Systems (NCES) are being developed to provide information and data services to all GIG users
 - Sensemaking is being enhanced through the development of a Horizontal Fusion portfolio
- Implications
 - These approaches may lead the way for an enterprisewide approach to the interoperability problem
 - However, issues remain on resources, governance, management, and culture

Institutional Initiatives: COTS Products

- Trend
 - OSD has issued policy directing the Services to make increased use of commercial standards and practices in the acquisition of new systems
- Implications on interoperability -- Uncertain
 - Plus: Military employment of accepted community-wide standards
 - Negative:
 - Rapid evolution of commercial products
 - Limited backward compatibility of COTS products
 - Mixed COTS packages may cease to be interoperable as new versions are released
 - Limited testing, documentation of COTS products

System Trends

- Trends
 - Introduction and refinement of the concept of an Object Request Broker (ORB) ('middleware'')
- Implications
 - May ameliorate interoperability problems associated with selected heterogeneous mixes of systems
 - However
 - There is a lack of universal standards among producers of commercial software
 - Commercial information systems are changing so quickly that rapid obsolescence is becoming common-place