IDA Research Notes

IDA Studies and Analyses Center

Spring 2006

NET-CENTRIC OPERATIONS

Issue Overview

The Department of Defense has embarked on a sweeping transformation of the military to fight tomorrow's battles as a joint force using network-centric operations. Generally, network-centric warfare is viewed in the context of improved situational awareness; speed of command; self-synchronized units; increased operational tempo; and an adaptable force. In simple terms, the output of net-centric operations is three-fold: the ability to post timely, relevant information; gain appropriate access to the information; and understand the information to make better decisions at every level of command. Command and control (C2) and networking underpin the ability to achieve this vision, and, as described in this issue of *IDA Research Notes*, IDA Studies and Analyses Center is making important contributions across a range of topics in this area.

IDA's work in C2 networking spans a diverse set of disciplines, sponsors, and challenges. To visualize the breadth of this work, it is useful to discuss the tasks in the context of DoD's major activities that are needed to bring capabilities to the warfighter: strategy, capability requirements, acquisition management, technology development, systems assessments, testing and evaluation, and operations.

In the strategy and capabilities area, we are working on several key tasks, including the Joint Battle Management Command and Control Roadmap. This effort focuses on providing logical methods for synchronizing interdependent C2-related programs into a coherent approach that is aligned to a unified strategy. The complexity of this task is compounded by the large number of programs and organizations that are developing, managing, and overseeing the work.

Systems and acquisition management are particularly busy areas for IDA's researchers in C2 networking. Our work includes innovative research on C4ISR systems that addresses the complexities and nuances associated with providing a meaningful cost estimate of systems that include intensive software, hardware, services, and information technology infrastructure.

The technology development and testing areas are best exemplified by our work on the Command Post of the Future (CPOF) and the Deployable Joint Command and Control (DJC2) system. These tasks focus on providing pragmatic tools for operational and tactical commanders. The CPOF system was accelerated through the development cycle and deployed to Operation Iraqi Freedom (OIF) so that it could be used to gain valuable experience and data in a live operational environment. Similarly, the DJC2 is being tested through training exercises in several commands.

IDA's analyses on the operational aspect of C2-networking through the OIF Bandwidth Studies were the first of its kind and provided a holistic look at the in-theater networks and the associated performance relative to the command structure down to the last tactical mile.

Lastly, our researchers have not only tackled tasks within these individual areas, but also across the whole problem set. Through an independent research project, a study team of senior researchers defined a potentially better approach by which the department could acquire C2-networking capabilities. The C2-Framework briefing provides a broad look at how the different decision areas are interrelated and some unique ideas on how to impact the decision cycle to ultimately improve the warfighter's capability to fight as a network-centric force.

IDA

4850 MARK CENTER DRIVE
ALEXANDRIA, VA 22311-1882
TELEPHONE (703) 845-2000

INSTITUTE FOR DEFENSE ANALYSES

IDA Studies and Analyses Center is a federally funded research and development center established to assist the Office of the Secretary of Defense, the Joint Staff, the Combatant Commands and Defense Agencies in addressing important national security issues, particularly those requiring scientific and technical expertise. IDA Studies and Analyses Center also conducts related research for other government agencies on national problems for which the Center's skills and expertise are especially suited.

Joint Battle Management Command and Control Roadmap Study

by Ronald Enlow

Joint Battle Management Command and Control (JBMC2) – the processes, architectures, systems, standards, and command and control operational concepts employed by the Joint Force Commander – optimizes the ability to manage the battlespace and inhibit the enemy's ability to function. To achieve this, the joint warfighter must be armed with interoperable systems that support mission success and reduce fratricide.

The JBMC2 Roadmap prescribes a way to achieve fully integrated capabilities that provide maximum interoperability of critical JBMC2 systems. This includes detailing several processes in order to derive JBMC2 capability needs; to identify the solutions to address needs; and to determine the appropriate mix of doctrine, organization, training, materiel, leadership, personnel, and facilities solutions. Finally, the Roadmap will help guide acquisition strategies in accordance with the Deputy Secretary of Defense interoperability goal of 2008.

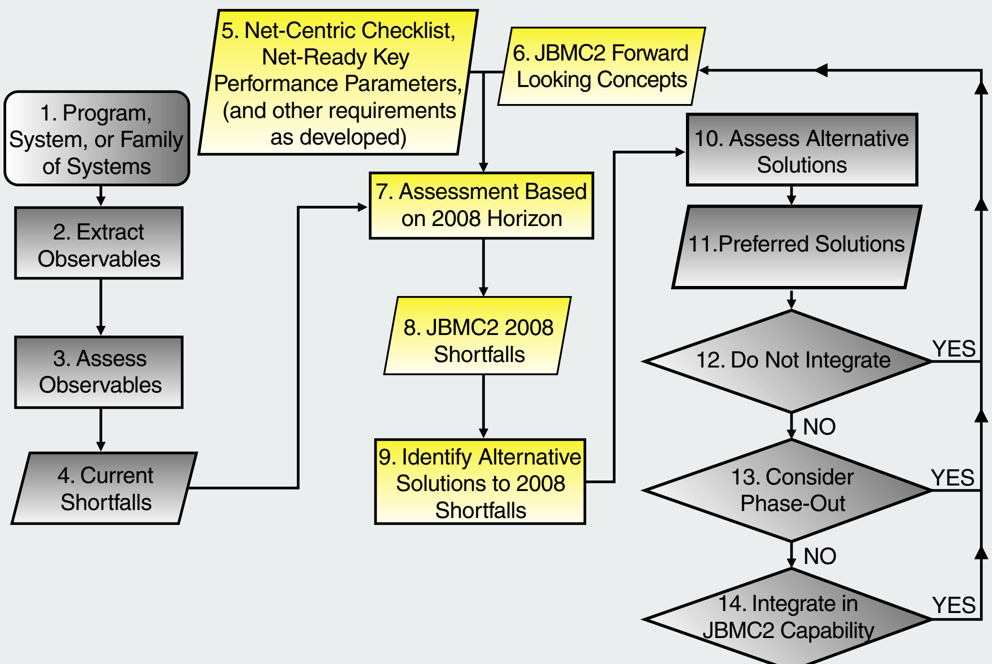

Figure 1. Capability Integration Assessment Methodology (CIAM) Flowchart.

DoD asked IDA to assist in developing a methodology that could help determine whether legacy JBMC2 systems could be integrated into the JBMC2, phased out, or not be integrated. The methodology was to be transparent, repeatable, and objective, and would focus on projecting interoperability by 2008.

Key participants in joint operations must be able to communicate and accurately pass information and data to each other and maintain effective organization, synchronization, timing, and a common interpretation of the battlespace. Interoperability is difficult to achieve when the warfighter is armed with disparate systems that were never designed to work together. The aggregation of the current Service systems inventory demonstrates that there are redundancies, single points of failure, and gaps in JBMC2 systems' ability to enable essential capabilities for the warfighter.

The methodology IDA developed, the Capability Integration Assessment Methodology (CIAM), was incorporated into the JBMC2 Roadmap Version 1.0 in May 2004. The methodology consists of the following:

- Phase 1 establishes the current interoperability status of the system under consideration and generates a list of current interoperability shortfalls.

Table 1. Program Assessment Tenets

Assessment Recommendations	Tenets
Consider Phase-Out	Not interoperable, neither cost effective nor mission-essential to make interoperable Not required once interoperable capability achieved Does not fit into future concepts of operation Cannot be made interoperable Is not planned to converge, and convergence would not be JMT essential
Integrate in JBMC2 Capability	Currently Interoperable with JBMC2 Not interoperable now but JMT-based need and cost-effective to make interoperable Soon to be (planned) interoperable, with mission need
Do Not Integrate	Service-unique application and no requirement for interoperability now or in the future, as drawn from JMTs and joint concepts

- Phase 2 projects the status of the program to JBMC2 in 2008, producing a list of future shortfalls and alternative solutions.
- Phase 3 assesses the alternative solutions and selects preferred solutions.

Based on consideration of the operational tenets, one of three recommendations is made (Figure 1 and Table 1).

Phase 1 of the CIAM process involves extracting and assessing program "observables," which cover a wide range of data sources, including operational lessons learned, concepts of operation, architectures, test reports, and Joint Capabilities and Development System (JCIDS) documentation. Table 2 illustrates a sample of the possible CIAM data sources and some generic potential shortfalls that might result from the assessments.

AFATDS CIAM Assessment

Soon after CIAM was developed, it was applied to two JBMC2 legacy systems: the Situational Awareness Data Link and the Advanced Field Artillery Tactical Data System (AFATDS). AFATDS provides automated fire support command, control, and communications to the Army, Navy, Marine Corps, allied forces, coalition forces, and selected foreign military sales customers. The system interfaces with 66 systems; there are currently 3,337 AFATDS systems in the field. To understand the interoperability required, the results from Phase 1 of the CIAM methodology show that AFATDS is interoperable with JBMC2, subject to the following: Future systems and system-of-system testing should

Table 2. Example Observables and Example Extracted Shortfalls

Observables	Extracted Shortfalls
Lessons Learned Exercises Experiments War Games	Identified operational deficiencies and interoperability gaps
Services Concept of Operations, Tactics, Techniques, and Procedures, Mission Need Statement, Operational Requirements Document Joint Concept of Operations, Tactics, Techniques, and Procedures, Operational Requirements Document, Capstone Requirements Document Architectures, Interoperability KPP	Unsatisfied information needlines, Information Exchange Requirement
Service Interoperability Testing JITC Interoperability Certification Developmental Testing & Operational Testing	Testing results
Initial Capabilities Document, Capability Development Document, Capability Production Document, Information Support Plan	Unsatisfied information needlines, Information Exchange Requirement

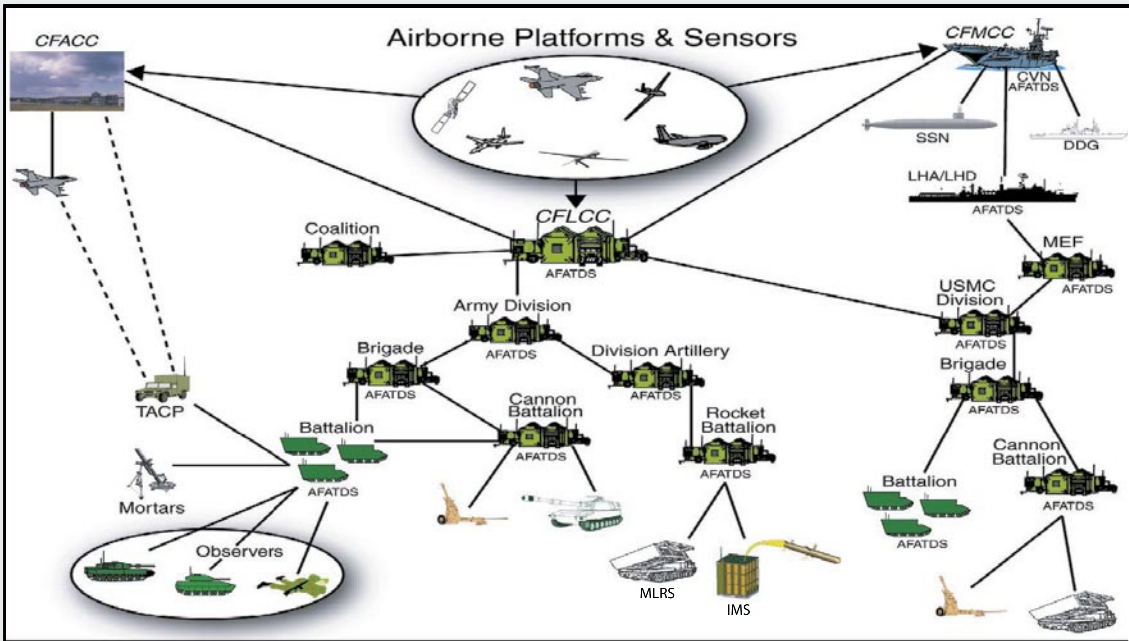

Figure 2. AFATDS Operational Architecture.

be identified and funded.

The AFATDS CIAM recommended proceeding with integration in the JBMC2 in three phases:

- Phase 1 – complete the system-of-system testing and documentation.
- Phase 2 – provide resources for the planned migration of AFATDS to Netcentricity.
- Phase 3 – produce a Capability Production Document or an Information Support Plan in accordance with Chairman of the Joint Chiefs of Staff Instruction 6212.01, Interoperability and Supportability of Information Technology and National Security Systems.

IDA costed the AFATDS recommendations in consultation with the project manager (Figure 2).

Estimating the Cost of Future C4ISR Systems of Systems

by David M. Tate

Command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) are the warfighter activities that enable network-centric operations and information superiority. The Office of the Director, Program Analysis and Evaluation, asked IDA to help estimate the costs of developing, procuring, and maintaining complex C4ISR systems of systems (SoS). IDA's review focused primarily on those costs that are not well captured by existing cost models of individual C4ISR components and systems.

Because C4ISR is about the creation, exchange, and exploitation of knowledge in the battlespace, certain technologies and subsystems tend to be recurring components and must be taken into account when determining costs. These include:

- sensors,
- communications infrastructure,
- data storage,
- data processing and analysis,
- computer networks,
- warfighter/machine interfaces, and
- artificial intelligence and decision support.

Cost Drivers

To predict the costs of a complex SoS, we start with the costs of the contributing systems. Some of the key cost drivers for C4ISR systems include:

- sensors,
- operational environment,
- size, weight, and power characteristics, and
- platform integration.

IDA also identified a number of important cost drivers that are not captured at the individual system level. These costs are often harder to anticipate and quantify because they are generally not associated with specific hardware and may span several programs.

Information Architecture. The purpose of any C4ISR SoS is to provide information services to war-fighters. The data-sharing and processing requirements within the SoS are determined by the set of services to be provided and the users of those services. For accurate cost estimation, the SoS cost model must identify the users and providers of all services, the frequency and intensity of potential service requests, and the communications paths and networks used by each service. The complexity and end-to-end quality of service required drives development, integration, and life-cycle costs throughout the SoS.

Data Requirements. Given the technical specifications of the SoS and the set of users and services to be supported, it is possible to calculate the data rates that each subsystem of the SoS must support to assure the needed services at the desired quality of service and availability. Data rate is a strong cost driver; at the cutting edge of available technology, doubling the available transmission rate may increase cost by a factor of ten. The costs associated with supported data rates are a function of the end-to-end services being supported and thus of the overall architecture of the SoS. This is especially true in a "meshed" network environment where local subsystems may be called on to serve as relays for information they do not use.

Data Fusion. When multiple elements of an SoS acquire independent data on a common topic, the data always disagree to some extent. Sensors are not identically calibrated; positions provided by global positioning systems have inherent small errors; different systems have different views of the same objects or events at slightly different times; and one sensor looks at an enemy vehicle while another listens to it. Resolving disagreements can be difficult, requiring sophisticated software and information exchange among participating subsystems. Developing the algorithms and implementing the software incur costs that would not apply to systems that acted independently on their own information.

Network Configuration and Dynamics. The size and complexity of the interoperating SoS, represented roughly by the number of nodes in the network that must share data and capabilities, are primary cost drivers. Hardware costs grow linearly in the number of nodes, but software design, testing, and systems engineering costs grow nonlinearly.

If the network involves mobile units or a varying set of nodes over time, the management problem is even more complex, and more network resources must be devoted to simply managing the network infrastructure. Less network capacity is available to carry information and so more bandwidth and higher data rates are required to provide a given level of service.

Security. Information assurance is a fundamental requirement of any military system involving the exchange of information. As a rule, the less flexible a communications channel is, the less complicated its information assurance needs to be. In a highly networked C4ISR SoS involving many services and many different types of users, the information assurance problem can become extremely complex. Multiple simultaneous levels of security, authentication of users in a mobile/dynamic network, and cryptographic algorithms for extremely high data rates are all expensive compared to traditional point-to-point communications security and transmission security.

Cost-Estimation Framework

Based on the cost drivers identified above, IDA developed a framework for estimating C4ISR SoS integration costs that follows a two-stage approach. Stage 1 performs a top-down survey of the architectural and information-exchange requirements characteristics of the target SoS and the services it provides. Stage 2 performs a bottom-up accumulation of costs, from the individual components to the highest SoS perspective, informed by the architecture and end-to-end data flow requirements discovered during the first stage.

The framework guides the development of a costing tool (or suite of tools) for C4ISR SoS cost estimation, including sensitivity analysis of key cost drivers. Because the costs of the contributing standalone systems (e.g., sensors, radios, networks, software) and components (e.g., processors, storage, antennas, power supplies, displays) are relatively well understood, IDA focused instead on the interactions among the networked systems in an SoS and how they affect the cost-estimating problem.

A C4ISR SoS cost analysis must start with an understanding of the details of the overall SoS architecture. These details include specification of all required data sharing within the SoS (and the services the data supports) as well as interoperability requirements with external systems (legacy and future) at each hierarchical level of the architecture. Once these integration and interoperability requirements are identified, they can be used to provide context for the Stage 2 local cost-estimation task at each level of integration in the SoS.

The Stage 2 bottom-to-top accumulation of cost components accounts for the individual systems as well as the interactions of the systems and subsystems (as informed by the overall SoS architecture) that drive the integration costs at each level. Costs at each level of integration will be driven by the nature of the integration, as well as by the subsystems to be integrated. Subsystem costs and characteristics can be known only by working from the bottom up, while the nature of the integration is implied by the architecture at each level. In extreme cases, entire platforms (e.g., low-observable or "stealth" aircraft) must be engineered as a unit to preserve global characteristics (low observability, noninterference of antennae, power, and cooling) while providing all necessary functions.

The Four-Level Model

IDA proposed a costing approach based on four notional levels of integration, from the lowest (subsystem) and to the highest (integrated network).

The first level is the integration of the subsystem. A synthetic aperture radar, for example, could include transmit/receive modules, antennae, receiver/exciter, a processor, back-end electronics, and possibly other items. Hardware costs at this level are straightforward, given the operational environment and performance requirements. Design, control software, and testing would be the primary integration cost categories, driven by physical interference and shared resource concerns. These can be expressed as a percentage of recurring hardware cost — typically about 10%, but sometimes more, depending on the specific subsystems and requirements involved.

The second level of is the integration of subsystems into suites, such as an avionics suite or a sensor payload package. The integration would involve a different set of physical interference and resource competition issues, as well as signal processing and fusion. Beyond the hardware cost, the main drivers would be design engineering, software, and testing.

The third level of is the integration of the suite of subsystems into the platform, such as the integration of an avionics suite and a sensor package into an airborne platform such as a UAV. These costs are highly variable, depending on what platform modifications must be made, what electronic interference must be controlled, how much room is available, and so on. This level has the most significant interactions between hardware-specific cost drivers and architecture-based cost drivers.

Note that for platforms at the cutting edge of technology, the platform design may be so tightly coupled with the various interdependent capabilities it must support that the entire platform is essentially one large "supersuite" of systems that must be designed as an integrated whole. This is common in such platforms as satellites, advanced fighter aircraft, and small UAVs. In these cases, the platform itself is a microcosm of the SoS design and costing problem. The techniques that contractors have developed for estimating the development and support costs of these platforms can potentially be generalized for use in the broader SoS context.

The fourth level of integration is the integration of the platform into the shared network. This would include the integration of an F-18 aircraft into the Navy Cooperative Engagement Capability, or an individual vehicle into the Army Future Combat System mobile network. This integration allows the platform to participate in the available networked services with other nodes on the network, such as airborne platforms and ground-based control centers. The cost of this integration has many dependencies. These top-level networking costs are almost entirely driven by the nature of the required collaboration, rather than by the details of the hardware and software on the platforms that will be collaborating.

The predominant type of cost (e.g., hardware, software, testing) will vary by level of integration. At the first level, hardware would be the primary cost, with integration of the subsystems accounting for approximately 10% of the recurring costs. Software, including embedded software, is likely to be substantial. However, the higher the level of integration, the less hardware contributes to overall costs, while design, software, management, and testing become relatively more important. Table 1 summarizes the cost breakdown for development costs.

Summary

In this work, we reviewed the nature of C4ISR systems (and SoS), the nature of their associated costs, and how both the nature of the systems and the nature of their costs are changing. We explored the cost implications of network-centric systems of systems and capabilities-based acquisition and proposed a two-stage C4ISR SoS cost-estimation framework, a top-down survey of the architectural and information exchange requirements characteristics of the target SoS, and a bottom-up accumulation of component, integration, and testing costs. For this study, we employed four levels of integration (subsystem, suite, platform, and network), but that structure can be modified. We identified key integration cost drivers (such as type of data dependency), key component cost driver (such as operational environment), and key architectural cost drivers (such as quality of service requirements). We also examined key organizational cost drivers such as requirements change management, and data requirements. Those findings have been reported separately.

Table 1. Cost Elements by Level of Integration

	Cost Element		
Level of Integration	**Hardware ("Boxes and Cables")**	**Software**	**Systems Engineering, Testing, and Integration-related Engineering**
1 (Subsystem)	Primary development cost	Secondary cost, (e.g., signal processing)	Consistent with 10% to 20% of recurring cost
2 (Suite)	Security cost, including hardware or interfaces and subsystem compatability (e.g., shared power data bus)	Secondary Cost	Primary cost, focusing on suite-level testing
3 (Platform)	Secondary cost, including hardware for environmental factors (acoustic, vibration, cooling)	Major cost fusion, decision support, displays	Primary cost, focusing on platform-level testing and ergonomics
4 (Network)	Minor cost, including compatible antennas	Major cost for network management algorithms, software radios	Primary cost, focusing on network-level testing and quality of service

Command Post of the Future

by George Lukes and Edgar Johnson

For more than five years, IDA has worked with the Defense Advanced Research Projects Agency (DARPA) to create a software environment and architecture focused on the needs of the tactical commander. In the first-generation digital command and control systems, commanders used acetate, voice shortcuts, sneaker nets, frame grabs, and PowerPoint to focus combat power. Now, however, DARPA's Command Post of the Future (CPOF) Program – a second-generation commander-centric software environment – provides ground force commanders greater situational awareness and distributed staff support, thus enabling faster and more effective decisionmaking.

CPOF enables division and brigade commanders to remotely collaborate and plan as they and their staffs work from individual PC-based work-stations networked in a distributed system. The initial CPOF system configured for division command included networked workstations for the division commander, division staff, brigade commanders, and brigade operations officers, and a liaison node at corps headquarters.

CPOF Capabilities

The technical challenge for CPOF was to create a software architecture based on three central tenets:

- Collaboration – creating a collaborative environment that would simultaneously produce a significant increase in situational awareness and understanding across the commander community.
- Visualization – enabling commanders to tune the supporting visualization systems in a way that best suits how they absorb information.
- Composability – creating an environment that allows commanders to operate using multi-modal interactions (speech and gesture) within the command system and, to a lesser extent, within the supporting control system.

CPOF was not designed to replace the tactical applications currently in use, but rather to serve as an information integrator, or battleboard, for the tactical commander.

The CPOF system maintains "liquid information" in a database format that separates data from the viewing space. As information enters the network, it takes the form of most meaningful to the commander. This enables faster visualization and optimal maintenance of large volumes of constantly changing information. Using a "databridge" front end, CPOF integrates input from commanders and staffs as well as real-time and near real-time feeds from numerous C4ISR applications. Shared awareness of the battlefield is provided by tracking the combat elements on electronic maps or satellite photos. Commanders no longer have to call on the radio to check the status of each unit.

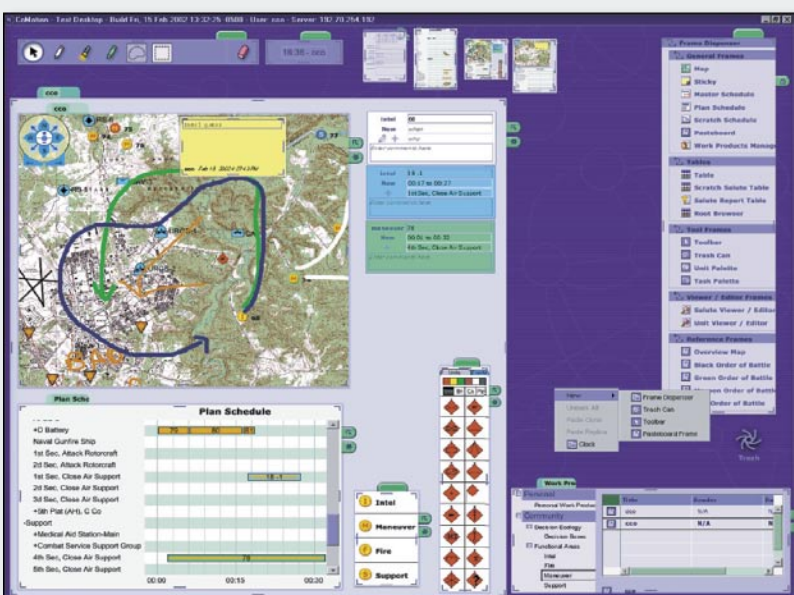

Figure 1. Typical CPOF Commander's Screen includes annotated map with Task Ink and Task Icons, Task Boxes, Planning Schedules, Tools, and Palettes.

CPOF supports advanced presentation-style briefings, including interactive maps, still photos, and video. Participants can sketch out their comments on the shared battleboard that can be viewed throughout the system (Figure 1). CPOF provides a commander-centric, scalable, reconfigurable environment that enables commanders to access all command post information and functions anywhere, anytime.

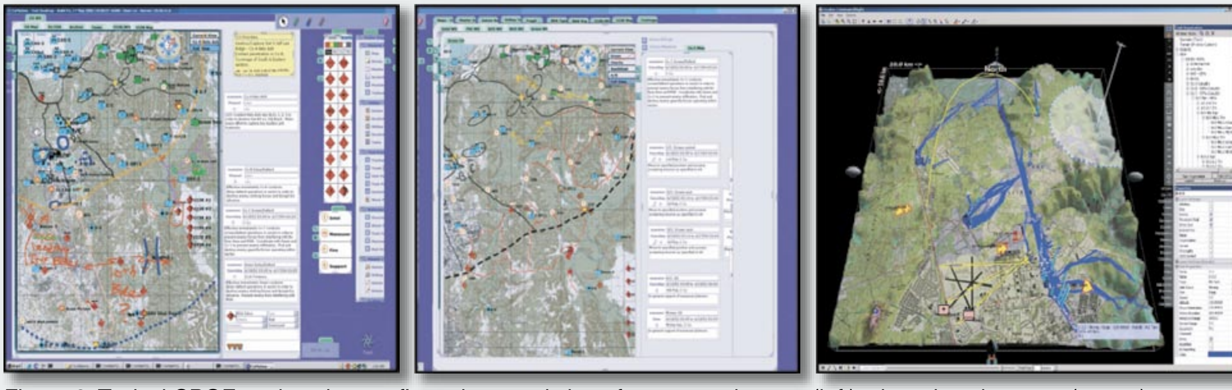

Figure 2. Typical CPOF workstation configuration consisting of a user workspace (left), shared workspaces (center), and interactive 3D visualization (right).

The Commander's Screen is also the medium for direct interaction between commanders and staffs. The map selectively displays Blue and Red forces, other annotations, explicit task boxes, and the planning schedule as well as available tools and palettes. The user can draw and highlight on the map where the graphics can be fixed, temporary, or momentary. Private workspaces are also available to all users.

A CPOF workstation supports three displays. Each user has a pasteboard or workspace that can be viewed by all (Figure 2, left window). Shared pasteboards or workspaces of other commanders and staff are organized by tabs (Figure 2, center window). These shared pasteboards are updated in real time. Other shared pasteboards include the Master Schedule, Sitrep Table, and the Salute Table.

The CommandSight module provides an interactive, three-dimensional picture of the battlespace that can be tailored by the user in terms of scale, perspective, aspect, background, and content with full access to data represented in the rest of the system (Figure 2, right window and Figure 3). Force structures can be displayed at levels of aggregation down to the entity level. A time slider and "snail trails" provide tools for visualizing forces over time. IDA research staff worked closely with developers in designing and populating the map display.

CPOF Development

The CPOF development has involved close and sustained interaction between three distinct communities: DARPA-selected, funded, and managed a set of world-class software developers; IDA consultants with distinguished command experience, serving as senior advisors and subject-matter experts; and active duty and retired command and staff officers participating in initial war games and subsequent "block parties" that were focal points in a spiral development cycle.

In fall 2003, the IDA team, led by BG Pat O'Neal, USA (Ret.), and MG Tom Garrett, USA (Ret.), coordinated CPOF's final test with the 1st Cavalry Division (1CD) at Fort Hood, Texas. Based on the success of these military utility experiments, the Army decided to deploy CPOF with the 1CD in March 2004 and the 3rd Infantry Division in 2005. For the initial fielding, members of the IDA team and CPOF developers worked on-site in Baghdad, while a reach-back facility was established at IDA.

Based on the operational success of CPOF in Iraq, a program of record was assigned to the Army's PEOC3T Acquisition community. Currently, there are more than 200 systems operating in Iraq with the 4th Infantry Division and the Multinational Corps–Iraq, and another 400 systems operating in Army and Marine communities and in the United States. In addition, U.S. Joint Forces Command has installed a number of systems to evaluate the utility of CPOF in the joint environment as part of its Urban Resolve 2015 Experiment.

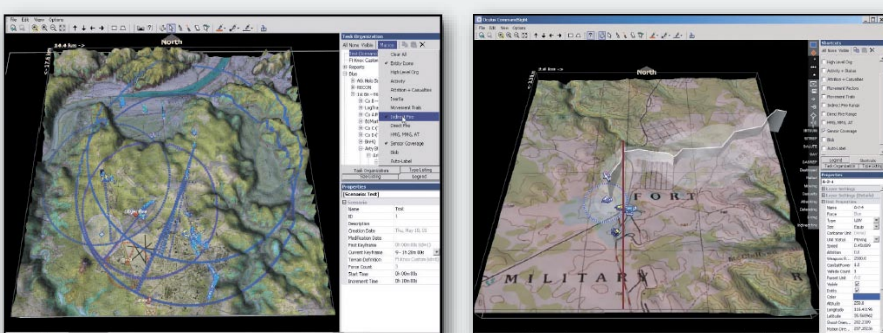

Figure 3. Tailored visualization using the interactive 3D CommandSight module.

Deployable Joint Command and Control System Testing and Evaluation

by Shawn C. Whetstone

The Deployable Joint Command and Control (DJC2) system – an Acquisition Category I Major Automated Information System program – provides joint force commanders with a common family of systems with which to plan, control, coordinate, execute, and assess operations. IDA involvement with the DJC2 spans multiple research divisions, including IDA's System Evaluation Division's analysis of alternatives for the Assistant Secretary of Defense Networks and Information Integration and the Department of the Navy, and continuing with the Operational Evaluation Division's support to Director Operational Test & Evaluation (DOT&E) for the test and evaluation of the system.

The DJC2 system is a suite of command and control applications (such as the Global Command and Control System and the Defense Collaboration Tool Suite), data systems, hardware (laptops, workstations, servers, and peripherals), networking (routers, switches, cables, and security components), supporting infrastructure (power, environmental control units, shelters, and furniture), mobility components (containers, transit cases, and pallets), and limited organic communications. Supported networks include the Secure Internet Protocol Network, the Non-Secure Internet Protocol Network, commercial Internet, and the Combined Enterprise Regional Information Exchange for coalition operations.

The system has three basic configurations: a 10- to 20-position En Route configuration, a 20- to 40-position Early Entry configuration, and a 60-position core configuration (Figure 1). Combining multiple core configurations creates extended (120 operational positions) and full (240 operational positions) configurations.

Test and Evaluation Program

IDA recommended that DOT&E support a test and evaluation concept derived from the operational mission and requirements of the DJC2: to provide the regional combatant commanders with a responsive, deployable joint command and control weapons system to fully command, control, and direct joint task force-level operations and perform the full range of their assigned missions (Figure 2). IDA's recommended concepts provided a foundation for Integrated Product Team meetings that developed an overall test strategy and the test and evaluation master plan.

The test strategy focuses on integration rather than on demonstrating the effectiveness and suitability of individual software applications. To establish operational effectiveness and suitability, IDA recommended a multi-Service operational test and evaluation that would deploy a joint task force with the DJC2 and that would execute operations consistent with the envisioned concept of operations. A series of focused events were planned to evaluate select portions of the DJC2 – from components of the supporting infrastructure and information technology through integration into a coherent system.

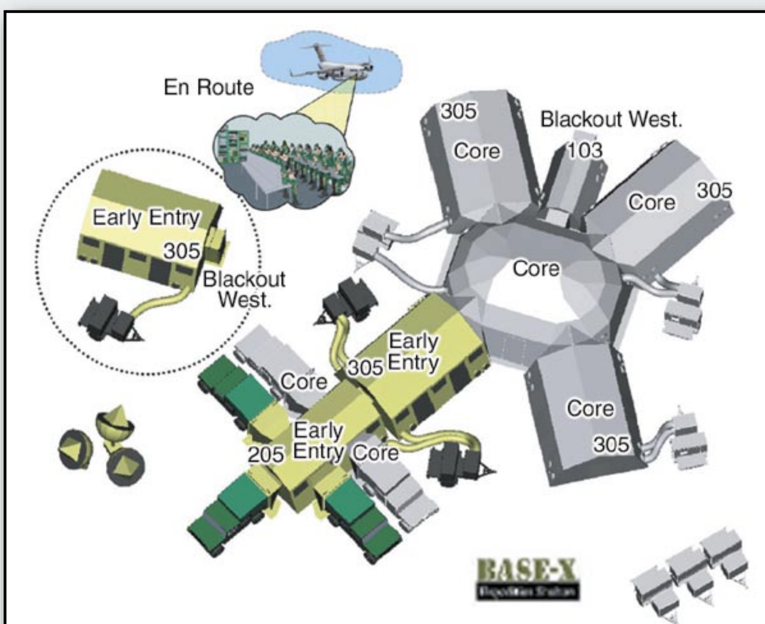

Figure 1. DJC2 Configurations.

The test strategy included early operator, tester, and evaluator involvement, with frequent testing to support the spiral development methodology. Rather than wait for a single final product, the products from early test spirals would be available to provide feedback to the integration effort. Also, to secure operator involvement and to satisfy the requirement for joint task force operations, the test concept used combatant commander training exercises as test event venues. This approach corresponds with increasing DoD interest in joint operations, in testing in joint environments, and in combining testing with training.

The DJC2 test program has completed a number of tests using operators from combatant commands participating in joint exercises. The operational evaluator also participates in all events including developmental tests. IDA researchers participated in the following DJC2 tests:

- Developmental test during the December 2003 Southern Command Exercise Purple Hurry to examine prototype shelters and infrastructure components.
- Developmental test during the February 2004 Southern Command Exercise Blue Advance in Honduras to examine prototype shelters and infrastructure components.
- Developmental and operational tests in June 2004 using a Mission Events List derived from U.S. Joint Forces Command Millennium Challenge Exercise to examine information technology and integration.
- Developmental test during the December 2004 Pacific Command Exercise Terminal Fury examining the complete DJC2, including information technology and deployability components (Figure 3).

Additional test events included:

- Developmental test during the May 2005 Southern Command Exercise Spanish Dragon examining the early entry and core configurations deploying and supporting Joint Task Force operations.
- Operational test during the September 2005 Southern Command Exercise Fuertes Defensas examing the early entry and core configurations deploying and supporting Joint Task Force operations.

The first four tests had staffs using the DJC2 in these tests act primarily as shadow joint task forces; the DJC2 received scenario information about support staff activities, but the staffs and their decisions did not directly influence the execution of the scenario. This approach provided operational context, scenario, and events to stimulate the activities of the operators while allowing data collection and controls more typical of developmental test events and early operational assessments. This also allowed the creation of a staff that included operators from each of the combatant commands, which permitted gathering a variety of views on how the DJC2 would support operations in different situations. The inclusion of various views is critical to support a DJC2 objective of providing a widely applicable standard command and control solution. The last two tests had operators from U.S. Southern Command's standing Joint Force Headquarters staff as the primary participants in the exercises. The Pacific Command provided support personnel and other combatant commands provided observers.

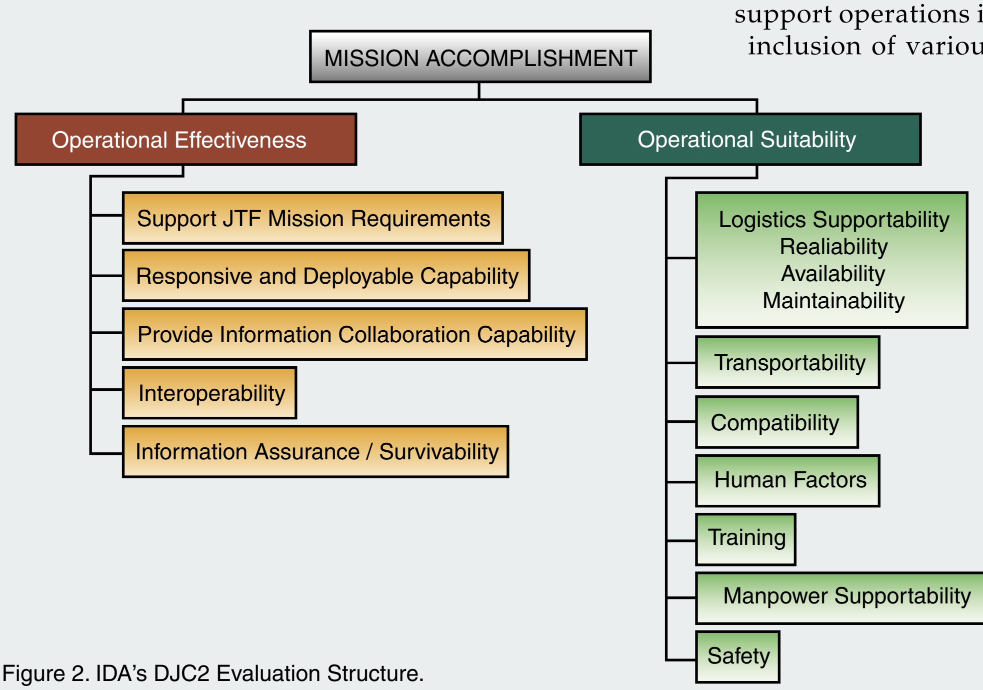

Figure 2. IDA's DJC2 Evaluation Structure.

Figure 3. Aerial View of the DJC2 Core Configuration Participating in the December 2004 Developmental Test CII (A) at the Naval Surface Weapons Center, Panama City, Florida.

Future test events include the following:

- Operational assessment during the March 2006 Southern Command Exercise Blue Advance to resolve critical operational issues regarding DJC2 ability to support joint task force operations.

- Multi-Service Operational Test and Evaluation during a June 2006 training exercise to establish operational effectiveness and operational suitability to support the beyond-limited-deployment decision.

The operators and support crew personnel in these two test events will consist primarily of the U.S. Southern Command's Standing Joint Force Headquarters.

Test and Evaluation Results

The operational concepts of the Standing Joint Force Headquarters and the capability provided in the DJC2 emphasize collaboration using software tools and remote connections rather than extensive face-to-face meetings. The tools supported with reach-back communications allow geographically and organizationally dispersed individuals to collaborate and share information to achieve the joint task force objectives. The DJC2 also supports the evolving organizational concepts for staffs such as dedicated knowledge management personnel.

In testing completed thus far, the missions given to the Joint Task Force element using the DJC2 information technology primarily have involved developing operational plans and monitoring the situation using procedures representative of the Standing Joint Force Headquarters with the collaboration, operational net assessment, and effects-based operations tools provided by the DJC2. The operators have successfully completed the planning tasks, collaborated, and developed plans using the available DJC2 tools.

A significant observable difference in the DJC2 operations is the nature of staff activities and noise level within the operations center. During DJC2 testing, staff members often remain sitting at their computer terminal throughout the majority of their shifts wearing headphones and collaborating electronically rather than moving about the operations center looking for one another. Consequently, the noise level and observable physical activity is lower. However, the collaboration tools and the ability to access information outside the operations center enhance operator productivity.

Involving the operational evaluators and operators executing operational scenarios early in the development and test process has provided numerous insights. The early tests helped refine requirements by identifying the need for simultaneous access to multiple networks and multiple computer workstations at each operator position to support their typical activities. Operator feedback supported selection of work area furniture and preferences for technologies for the large-screen displays throughout the operations center. The events also provided insights for practical concerns such as storage space for personal gear, notebooks and reference materials, and the need for a location within the operations center to hold face-to-face discussions. Overall, the operator feedback has been generally positive regarding provided capability and the effort to standardize command and control.

The test program also highlights the need to consider logistics support and training aspects during development. Emphasis is often placed on acquiring and fielding the latest technologies. Involving the warfighters early in the development highlighted that operators are concerned not only with receiving the technology, but also with the ability to sustain the equipment and maintain proficiency after the initial fielding. Providing accurate and complete documentation, technical manuals, and user manuals are essential for successful deployment of any new system.

Summary

The DJC2 is successfully executing an aggressive spiral development to deliver an integrated deployable command and control capability to the combatant commanders. The test strategy includes operators in an operational context to the extent possible. The nature of the DJC2 and its intended users requires integration into joint events and participation in large-scale training exercises. The nature of the participation is tailored to the test objectives ranging from providing a mission events list to acting as a shadow joint task force to eventually being a primary joint task force element. The continually evolving nature of command and control technology and operational concepts requires including operators and testers early and throughout the development to field technologically and operationally relevant systems. Cooperation among the DJC2 Program Office, the Joint Forces Command, the combatant commanders, and DOT&E has supported the test strategy and demonstrated the value of including the test and user communities throughout the process. IDA will continue providing analytical support for the test and evaluation of the DJC2 and will document the lessons learned to improve the acquisition and testing of future command and control systems.

Operation Iraqi Freedom Bandwidth Analysis

by Robert Rolfe

The Joint Center for Operation Analysis and Lessons Learned (JCOA-LL) asked IDA to identify communications bandwidth lessons learned based on the communications architecture used during major combat operations of Operation Iraqi Freedom (OIF). This study takes into account specific systems and capabilities from the edge of the joint integrated network and command infrastructures to the "last tactical mile" (LTM) and deployed user. IDA was asked to perform the following:

- Describe the OIF communications architecture in narrative terms.
- Assess bandwidth for OIF area of regard down to the LTM and global reach-back.
- Assess bandwidth differences among Services in terms of capacity and usage.

JCOA-LL collects, analyzes, and archives relevant lessons learned from the operational level of war in support of regional combatant commanders. In this case, JCOA-LL's analysis concerning OIF was for the Secretary of Defense and the Combatant Command. These analyses provide operational documentation from the warfighter that often result in recommendations for change to current plans and policy.

The Process

IDA proved the ideal organization to conduct this analysis. The study required unfettered access to the JCOA-LL database and critical IDA Joint Advanced Warfighting Program (JAWP) facility resources essential to data collections, which were not released outside JCOA-LL's control. Because of other JAWP activities, IDA already was providing some support across the spectrum of information and resources needed for this study

IDA's initial analysis focused on the communications architectures and bandwidth capacities at the fixed and stationary sites, starting with the headquarter locations of the Joint Command and Control Centers within the OIF area of regard. With that as the foundation, the analysis followed the information flow through the Service communication infrastructures by focusing on

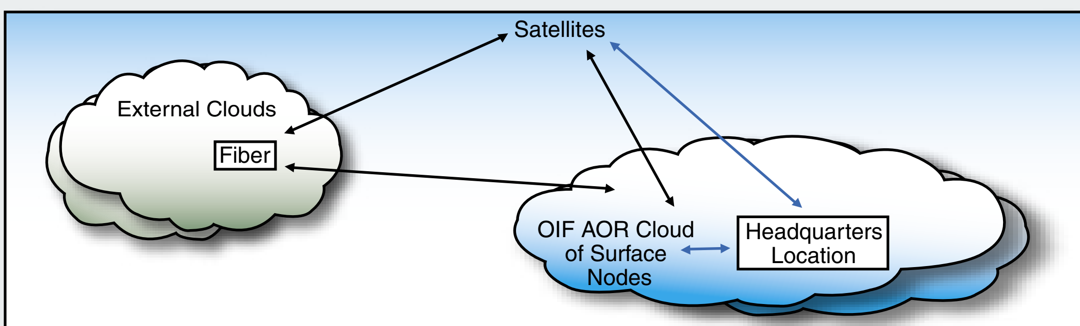

Figure 1. Determining Communications Bandwidth Capacity by Type (Fiber & Satellite), connections to Operation Iraqi Freedom area of responsibility (AOR) Cloud of Surface Nodes, and Headquarters. The figure above illustrates the bandwidth elements of the OIF communications network. The total bandwidth is the sum of all of the long distance communications links connected into a network. The network of interest is within the AOR of the U.S. Central Command and external (e.g., CONUS). We illustrate both terrestrial fiber connections external to and within the AOR and links through satellites. The slender black lines are possible connections, and the blue line is an example of connections to a headquarters. A cloud is a collection of network nodes that may provide connectivity within the set of cloud nodes and connectivity to other external clouds and nodes.

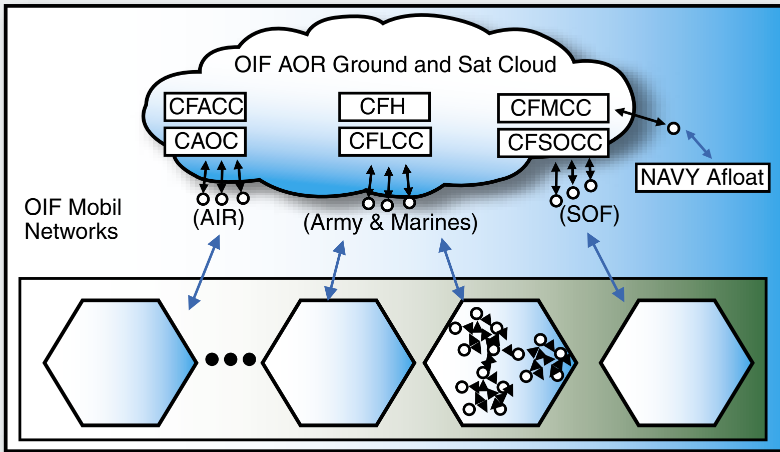

Figure 2. Analyzing Communications Bandwidth Capacities to the Mobil Networks by Command Centers and Services. The figure above illustrates the quasi-stationary nodal command centers in the AOR and how they connect to joint Service mobile networks or nodes. The blue lines represent many connections.

acquisition and operations. The final IDA report was released to the sponsor in the 2nd quarter of FY2006, and continuing efforts are addressing current OIF Army and theatre coalition networks and Tsunami Relief Operations networks. Additional effort to support U.S. Central Command strategic architecture activities is currently being defined, and IDA is briefing organizations and agencies across DoD.

specific capabilities of individual terminals and networks (Figures 1 through 4).

The study team located and collected sparsely available information, reverse-engineered communications architectures to a reasonably high-fidelity, and characterized in measurable terms the LTM communications capabilities and limitations. JCOA-LL has used IDA's study to create input for the concept refinement phase of for future network acquisition through JCIDS process, including to the JROC to support new requirements, and the Network Centric Warfare Functional Capabilities Board. An annotated briefing of IDA's analyses has been presented as "predecisional information" across DoD organizations responsible for future network

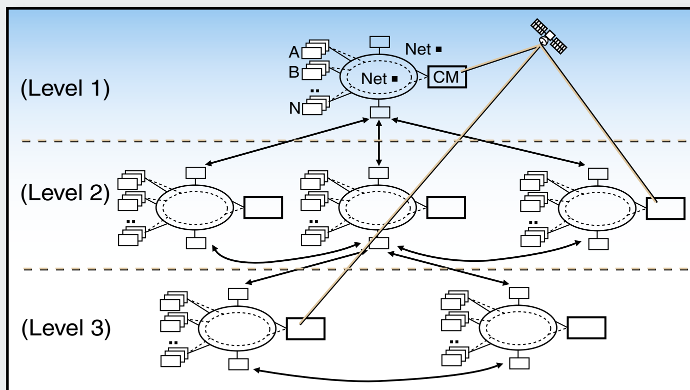

Figure 3. Characterizing Specific Bandwidth Capacities by Terminal and Networks Employed at Various Echelons. The figure above illustrates echelon-level networks and their connectivity to other echelons by direct line of sight connections (in black) and satellite connections (in gold) across echelons.

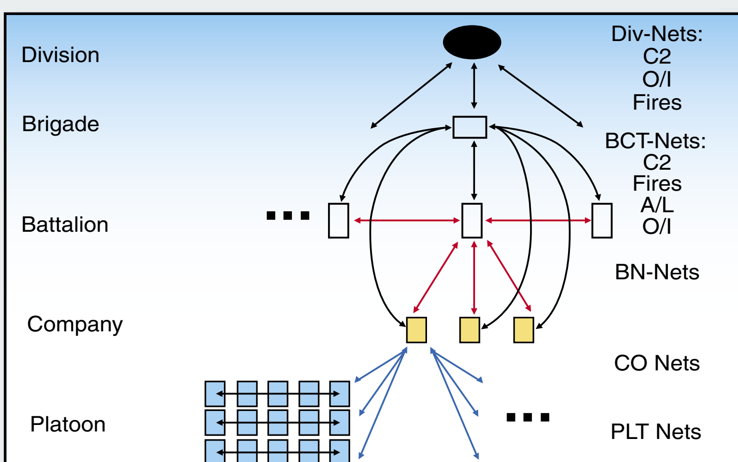

Figure 4. Examples of Typical VHF Radio Nets Identified in Use During OIF Major Combat Operations. The figure above illustrates echelon-level networks and their connectivity to other echelons by direct line of sight connections (in black) and satellite connections (in red) across echelons.

Framework for Achieving Joint Command and Control Capabilities

by Richard Ivanetich

Effective command and control (C2) is essential for joint U.S. military operations. Numerous efforts to enhance C2 are ongoing across DoD, but they are often spread over many organizations and are not always coordinated. Generally, these efforts result from three different perspectives – visionary, acquisition, and employment – that should be more fully integrated in order to achieve enhanced C2 capabilities.

IDA Studies and Analyses Center created a cross-divisional working group, consisting of approximately a half-dozen research staff, to share their differing perspectives and to synthesize a unified "IDA perspective" that proposed a framework for a more integrated approached to achieving joint C2 capabilities. The group's intent is to help DoD develop C2 capabilities and to build on, not duplicate, DoD's many ongoing planning initiatives. The work, completed in fall 2004, has been briefed to senior Department officials, and the concepts subsequently have been refined under sponsored research efforts.

Developing Joint C2 Capabilities

The working group began by synthesizing into an overall process the various component processes that contribute to DoD's development of joint C2 capabilities (Figure 1). In addition to considering the processes within each of the major blocks – Capability Needs Definition Processes, DoD Vision and Strategic Goals, Resource Allocation Process, Program Definition and Execution, and Rapid Capability Insertion Processes – the study focused on the interfaces between these major blocks (the arrows crossing between the blocks). Improving these interfaces means better integration across the different perspectives. This analysis then identified five topics to enhance integration.

Developing a Mission-Based C2 Capabilities Framework

Examining the interfaces began by considering the interaction of the DoD Vision and Strategic Goals block with the adjacent blocks. Those interfaces are characterized by multiple vision statements, which do not provide adequate guidance for integrated program development. IDA concluded that a mission-based capabilities framework was needed to determine which goals and priorities could be established. To this end, the team proposed adopting a mission set across the joint community to structure mission analyses

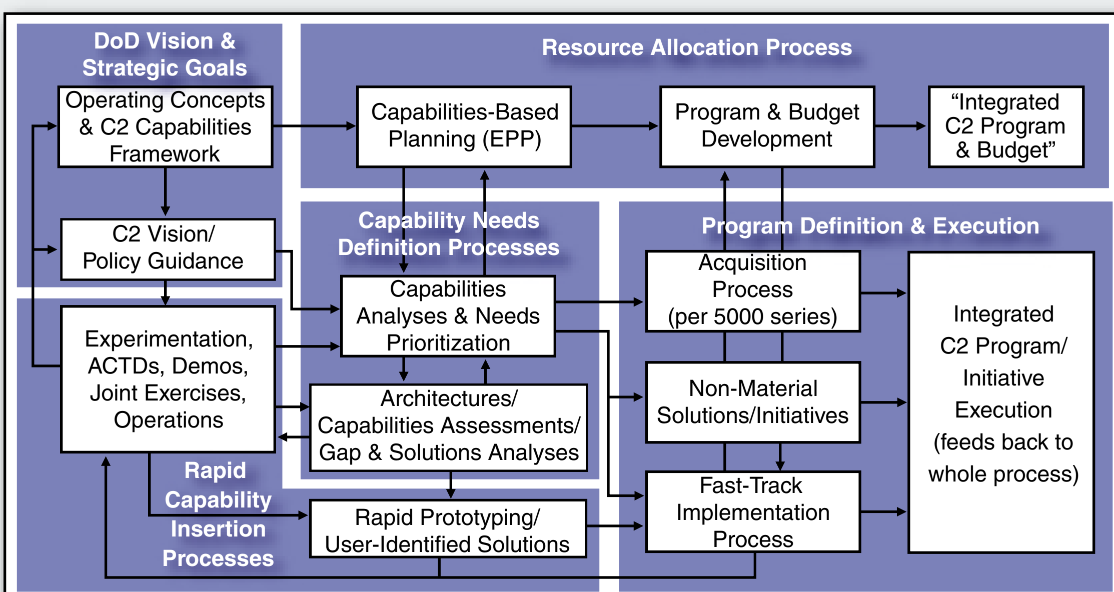

Figure 1. Process for Developing Joint C2 Capabilities.

Mission Set	Mission, Tasks, and Doctrine Publications *
Synchronization of Maneuver and Fires	■ Fire Support 3-09 ■ Targeting 3-60 ■ CAS 3-09.3 ■ Interdiction 3-03 ■ Information Operations 3-13
Engaging Time-Sensitive Targets	■ Targeting 3-60 ■ Interdiction 3-03 ■ Commanders' Handbook for Joint Time-Sensitive Targeting ■ Information Operations 3-13
Theater Air and Missile Defense	■ Countering Air & Missile Threats 3-01 ■ Aerospace Defense of North America 3-01.1 ■ OCA/DCA 3-01.2/3-01.3 (in preparation), JSEAD 3-01.4 ■ Theater Missile Defense 3-01.5 ■ Info Operations 3-13
ISR Tasking, Dissemination and Integration	■ Intelligence Support to Military Ops 2-01 ■ JTTP for Intelligence Support to Targeting 2-01.1 ■ JTTP for Intelligence Preparation of the Battlespace 2-01.3
Forcible Entry	■ Forcible Entry Operations 3-18 (covers airborne/air assault/amphibious ops) ■ Information Operations 3-13 ■ Amphibious Ops 3-02 ■ Landing Force Ops 3-02.1
Dynamic Deployment & Reception Planning	■ Defense Transportation System 4-01 ■ Movement Control 4-01.3 ■ JRSOI 4-01.8

* representative list of missions, tasks, and doctrine publications for major combat operations.

Figure 2. Composite Sets to Structure Mission Analyses.

(Figure 2). Fundamental to this mission perspective is that attention be given to joint C2 through the tactical level.

The study team is not suggesting that the mission set is exactly the right one, but rather that some relatively small set of missions should be chosen to organize thinking about C2 mission functionality. As different elements of the overall community conduct C2 analyses and development, they will have a common mission framework through which to relate their efforts.

Articulating the Role and Use of Architectures

When the working group considered the interface of the Capability Needs Definition Processes block with its adjacent blocks in Figure 1, it concluded that the output of those processes is not synchronized with the resource allocation and program definition processes. To enhance that synchronization, the study proposed using a mission framework (as described above), architectural analyses, and a systematic approach to understanding net-centric capabilities.

The use of architectures in DoD has a mixed history. On the one hand, they provide a basis for achieving consensus on defining required operational capabilities, conducting systematic investment planning, and harmonizing near-term activities and long-term goals. On the other hand, architectures are often difficult, costly, and time-consuming to develop and maintain; are frequently lacking sufficient guidance on the detail needed; and are typically too complex for DoD leadership to work with. Still, the study team strongly favored using architectures, based on its experience in other work developing and applying architectures. Figure 3 presents an outline of the methodology that IDA developed in that work.

Developing the operational views and technical views of the architecture required significant analyses. What is unique, however, is that those operational and technical views are not products in themselves, but are applied to produce a roadmap investment strategy. IDA has applied this methodology to plan development for combat identification, joint close air support, and joint Blue force situational awareness.

Based on that work, IDA recommended the following principles for applying architectures:

- Limit architecture scope and detail to intended use, focusing on developing a few good architectures to start.
- Emphasize mission focus.
- Strengthen capabilities

assessment by U.S. Joint Forces Command and the Services.

- Institutionalize a Capabilities Roadmap and Investment Strategy methodology (Figure 3) and integrate it into the DoD planning process.
- Evolve architectures as operational concepts, requirements, and solutions mature.

Relating Net-Centric Concepts and Technical Capabilities

To assist in establishing a systematic basis for analyzing the particulars for given missions, the study team characterized the "space" of net-centric operations (Figure 4). Analyses must be conducted for all points in the space to understand the extent of operational capability at a level of command that can be realized from technical capabilities. For example, if given technical capabilities are available for network connectivity, data sharing, and enterprise services, how much shared awareness can be achieved at the operational level? Or vice versa, given a desired degree of shared awareness, what measure of each of the three technical capabilities is necessary? This systematic set of analyses does not appear to exist. Analyses at the tactical level are particularly necessary because of stressing demands imposed there – low latency, data accuracy, and limited/intermittent connectivity. The study team made two general recommendations for developing net-centric C2 capabilities:

- Increase operational-technical interaction, with a tactical focus. While there has been impressive net-centric application of existing technical capabilities in recent military operations, there appears to be little thinking at the mission level in the operational community about applying anticipated future technical capabilities.
- Use an evolutionary approach to achieving net-centric capabilities. Elements of this approach include selecting initial mission areas to provide focus; employing integrated architectures for each area and refining them based on results from experiments and exercises; working systematically through the space of net-centric operations (Figure 4); and using the knowledge gained to guide system development and deployment.

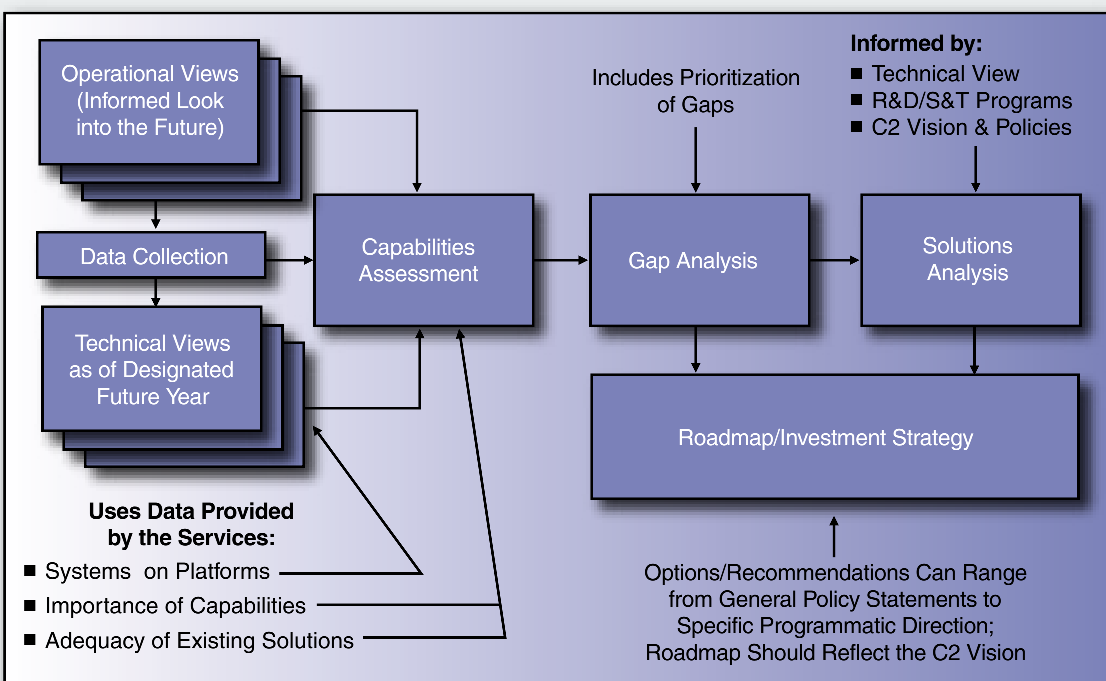

Figure 3. Capabilities Roadmap and Investment Strategy Process.

Facilitating Rapid Capability Insertion

The last set of interface considerations for the overall process pertains to the relation of the Rapid Capability Insertion Processes block with all the other blocks. Given that forces may have to fight at any time in the current world environment, near-term needs and long-term objectives must be balanced. However, the rapid capability insertion process is only weakly supported by the remainder of the overall process. Senior officers have indicated that capabilities are often achieved by "work-arounds" and personal efforts by senior combatant command (CoCom) members. Rapid capability insertion requires stronger coupling to the rest of the process without unduly centralized control, which would impede the rapidity of insertion.

The study team suggested that CoComs continually promote prototyping and fielding to achieve rapid capability insertion. The idea is to develop a process responsive to the rhythms of operational challenges and technical opportunities and that would not be tied to some fixed planning and programming cycle. CoComs conduct exercises, ranging from table-top ones to those involving the large-scale deployment of forces. These exercises (and possibly preparation for and conduct of actual operations) would be used to bring together operators and developers; incorporate demonstrations, experiments, testing, and training; systematically capture mission and system performance results that are fed back to operators and developers; remedy deficiencies and continue prototype development and fielding; and identify means to sustain the deployed capabilities. With this process in mind, the working group recommended CoComs do the following to enhance rapid capability insertion:

- Institute a rapid spiral process in conjunction with their exercises, with support from Services and agencies.
- Develop rolling "500-day" plans to guide execution of the rapid spiral process in order to address their priority joint C2 challenges.
- Have staff to carry out the spiral development process, using a small elememt for overall management and the Services and Agencies for help with execution.
- Obtain funding to conduct the spiral development and field prototypes that is flexible enough to be applied to needs and opportunities as they arise.
- Create operational and technical teams that worked across CoComs to share innovations.
- Align prototype developments in each CoCom with an overall net-centric architecture to allow interoperation of capabilities when deployed across theaters.

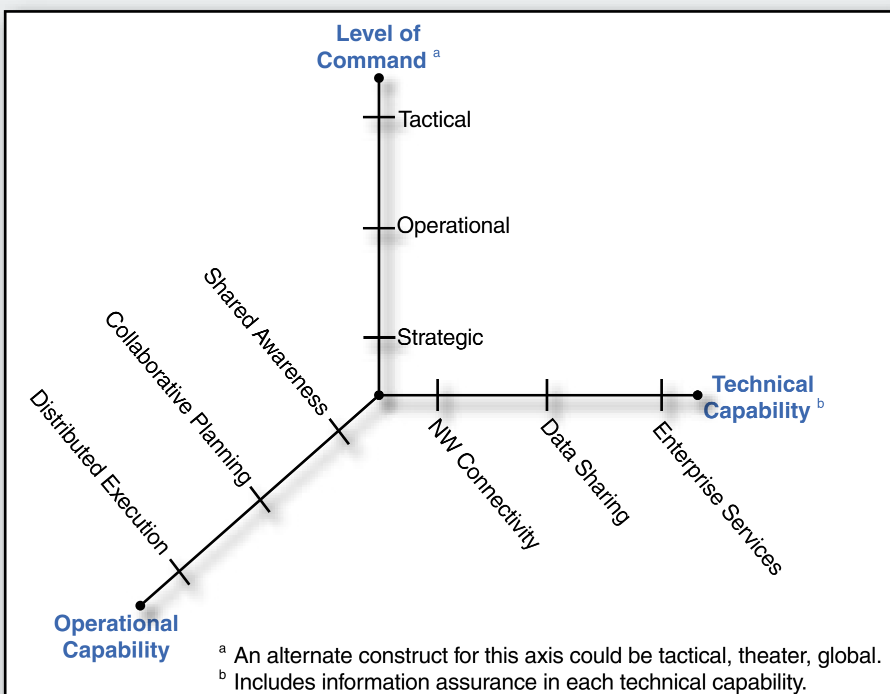

Figure 4. The Space of Net-Centric Operations.

Establishing a Near-Term 'Business Plan'

The last step toward synthesizing and capturing the output of each of the previous four elements is to develop a "business plan," which would include an understanding and awareness of ongoing activities and a link with resource allocation. The plan would aid senior-level decision-making and promote common understanding throughout the community. It would commit to near-term C2 improvements and relate to longer-term developments. The business plan should include one chapter for each composite mission area (Figure 2) and a separate chapter for the Global Information Grid, which provides capabilities across all mission areas. Each chapter would provide the following:

- A summary of joint C2 vision and goals.
- A description of ongoing and planned activities – architecture development, rapid capability insertion activities, and formal C2 programs.
- A summary of resource commitments both to enhance visibility by relating resources programmed in the near term to high-priority mission needs and to allocate to CoComs rapid capability insertion funding to reduce critical near-term operational risks.

The plan would complement and draw from other ongoing planning initiatives (e.g., Functional Capability Board analyses, roadmap development).

This effort would have to be initiated by the Deputy Secretary of Defense, who also would assign the leads for the overall plan and its major parts. Generating such a business plan would be a substantial undertaking, and so it may be helpful to first develop a pilot plan to assess the feasibility of developing the larger plan, the utility of the product, and its relation to existing DoD planning processes. A pilot plan might, for example, address only one of the composite mission areas and the Global Information Grid.

Summary

The working group identified the following four ways to improve the process for developing joint C2 capabilities:

- Use a mission-focused perspective to guide C2 capabilities development.
- Employ architectures to drive necessary analysis and promote community consensus.
- Tie together the development of net-centric concepts and the underlying technical capabilities.
- Support a decentralized CoCom-driven process for rapid capability insertion.

In addition, the group proposed using a joint C2 business plan to capture and commit to the results of the C2 capabilities development process.

Other IDA Headlines

Medical Care Cost Growth

IDA is helping DoD estimate the impact of "ghosts" – retirees and family members who had private health insurance but who are now returning to military-provided coverage under TRICARE. The increasing numbers of these returning retirees is largely due to rising private-sector insurance premiums and other out-of-pocket expenses. IDA analyzed data from DoD surveys and health care claims to estimate models of insurance choice, utilization, and unit costs. Using these models and existing forecasts of private-sector economic trends, IDA predicted that DoD health care costs will continue to rise, but at a decreasing rate. IDA is now extending the analysis of TRICARE "ghosts" to include other beneficiary groups and sources of cost growth.

VA Compensation Study

IDA has been asked to help the Department of Veterans Affairs (VA) determine why there are differences in the VA's average monthly disability compensation payments made to veterans living in different states. IDA will conduct a study using statistical models of the major influences on compensation payments that will develop baseline data and metrics for monitoring and managing variances. The study will continue IDA's seven-year history of providing the VA with analytical analysis and support.

Rotorcraft Survivability

A recent assessment of rotorcraft operations in Afghanistan and Iraq identified the root cause of approximately 100 rotorcraft losses that have occurred since the fall of 2001. Our researchers found that two-thirds of these losses are attributed to mishaps caused by degraded visibility, and the remaining losses came as the direct result of enemy engagements, primarily from MANPADs, rocket propelled grenades, and small arms. We assessed materiel and tactics-based solutions for reducing rotorcraft losses and prioritized ways to improve the safety and survivability of the current rotorcraft fleet.

Integrated Cross-Capability Assessment and Risk Management Framework

IDA has developed a decision aid – the Integrated Cross-Capability Assessment and Risk Management (ICCARM) risk assessment methodology – that DoD can use to rapidly evaluate how well the future year defense program and other resource alternatives mitigate and balance strategic risk across all major elements of the national defense strategy. Strategic risk is the damage to the national interests expected to result from relying upon a given overall U.S. force. Specific calibrated consequence and likelihood scales are used to conduct the risk assessments. During the Quadrennial Defense Review, IDA used this methodology to obtain from more than two dozen senior DoD, military, and civilian decision-makers their not-for-attribution evaluations of the strategic risks the United States would be exposed to if DoD continues to rely on the future programmed force in the period 2010-20. Results of these risk assessments have been briefed to many senior DoD officials, including the Chairman of the Joint Chiefs of Staff and the Deputy Secretary of Defense. A briefing is now being scheduled for the Secretary of Defense, both on the baseline assessment and to propose ways to institutionalize strategic risk assessments for top leaders in the department.

Terrorist Perspective Project

A team of civilian and military analysts from IDA's Joint Advanced Warfighting Program is extracting strategic and operational insights from the perspectives of the Salafist Jihadists — al Qaida and its associates. The team is drawing on thousands of translated documents (captured and open source), information from detainees, and graphic materials. What emerges is a candid look at the enemy's strategic thoughts and self-image. This study will contribute to the United States' ability to prosecute the war by allowing us to understand better enemy's actions and to operate directly against the enemy's self-perceived weaknesses.

National Information Assurance Partnership Review

An IDA research team has completed a comprehensive review of the National Information Assurance Partnership (NIAP) to determine its efficacy and to determine if the processes it has implemented help in the nation's information assurance efforts and the national cybersecurity posture. A draft report provides the Department of Homeland Security's Information Analysis and Infrastructure Protection Office and DoD's Defensewide Information Assurance Program six options for implementing the NIAP functionality that range from elimination to complete revision of goals and methods. We will be working closely with DHS and DoD to implement ways to improve the nation's ability to work with industry to produce more secure commercial IT products.

Developing a Global Information Grid Architecture

IDA continues to play a leading role in the development of Global Information Grid Architecture elements and processes for the Assistant Secretary of Defense for Networks and Information Integration. Our work centers on the development of the Netcentric Operations and Warfare Reference Model (NCOW-RM), which provides a common reference tool that enables the depiction and relationship of other architectures and features across many systems, programs, and operations. Our researchers lead the development of the NCOW-RM, which includes not only constructing the actual reference model, but also the performance measures, taxonomy, ontology, and interfaces with other architectural frameworks.

Chem-Bio Non-Standard Equipment Review Panel

The Chem-Bio Non-Standard Equipment Review Panel ensures that civilian equipment purchased by DoD for non-battlefield applications is suitable for its purposes. In many cases, established standards of performance for such equipment do not exist, and the Panel evaluates the equipment on the basis of its intended use and the results of independent tests that have been performed. We are performing independent technical reviews of information packages submitted by the Service and agency proponents of items of chemical and biological defense equipment to determine whether they are safe, effective, and suitable for their intended use. Our findings are considered by the Panel as it decides whether to approve the submission, allowing Services or Agencies to employ the equipment, reject the submission, or request additional information.

Review of FCS Key Performance Parameters

We have been reviewing performance metrics related to the Future Combat System's key performance parameters, particularly metrics that might cut across the performance parameters. One such parameter, transportabity, led to a derived requirement for compatibility with C-130 transport for 250NM (500NM objective), which constrains the weight to 20 tons or less. Our review found that constraining the weight to 20 tons to ensure C-130 compatibility offers no advantage for unit mobility. However, survivability against kinetic energy rounds from widely proliferated 25-40 mm cannon falls dramatically as vehicle weight drops from 30 to 20 tons.

Nuclear Proliferation Studies

IDA is assisting DoD in addressing concerns regarding nuclear proliferation. The Deputy Assistant to the Secretary of Defense for Chemical Demilitarization and Threat Reduction has asked IDA to look at the problem of monitoring nuclear proliferation. We are developing approaches and assessing technologies that might exploit indicators of nuclear proliferation that are independent of the possibility of a test. We are also assisting the Deputy Assistant to the Secretary of Defense for Nuclear Matters in preparing and coordinating a capabilities-based assessment (CBA) of the physical security of nuclear weapons in DoD custody, both in the United States and abroad. The CBA, the first step in the JCIDS process, analyzes capabilities, needs, and solutions.

Selected Articles from Past Issues

Systems Evaluations

- AIM-9X: A Modeling and Simulation Success Story *(2001)*
- Assessment of Airlift Requirements *(2000)*
- Assessment of Lethality Enhancement Alternatives for the AC-130 *(1999)*
- COATS: A New Approach to Submarine Testing *(2003)*
- Evaluation of Long Range Fire Support Systems *(1998)*
- Evaluation Plan for the Navy's Area Theater Ballistic Missile Defense System *(1997)*
- Integrated C4ISR Analytical Tool Set *(2001)*
- Naval Expeditionary Warfare Maneuver, Planning, and Execution *(2003)*
- New Initiatives for Operational Test and Evaluation *(1999)*
- Realistic Testing: Key to F-22 Mission Effectiveness *(2002)*
- Simulation in Support of Live Fire Test & Evaluation *(1999)*
- Small Combatants: Implications for Effectiveness and Cost of Navy Surface Forces *(2003)*
- Strategic Airlift: IDA's C-5 Modernization Study *(1998)*
- Surface Ship Radars *(2003)*
- Testing the Navy-Marine Corps Intranet *(2003)*

Technology Assessments

- Advanced Distributed Learning (ADL) *(2000)*
- Assessing the Future of the Global Positioning System *(2000)*
- Defense Electronics: Keeping the Edge *(2000)*
- Digital Representations of the Environment: Requirements, Representations, and Constructions *(2000)*
- IDA Support for the Global Combat Support System *(2000)*
- IDA Hosts Workshop on Advanced Technologies and Future Joint Warfighting *(1999)*
- MicroElectroMechanical Systems – Prime Enablers of Future Weapons Systems *(1998)*
- Militarily Critical Technologies Program *(2004)*
- Quantifying Military Information *(2001)*
- Smart Materials and Structures… or "It's a bird! No, it's a plane…" *(1999)*
- Technology and the Challenges of Defense Training *(1999)*
- The MOUT ACTD Analysis and Technology Assessment *(2000)*
- Warfighters' Edge: Using Intelligent Agents to Solve Warfighter Problems *(2002)*

Resource and Support Analyses

- Cost Analysis for the Airborne Electronic Attack Analysis of Alternatives *(2003)*
- Cost Estimating for Next Generation Aircraft *(2000)*
- IDA Builds Capability to Evaluate Industrial Base *(1998)*
- IDA Course Strengthens Acquisition Workforce's Understanding of Operating and Support Cost Analysis *(2002)*
- IDA's Role in the President's Commission on Critical Infrastructure Protection *(1997)*
- Idle Capacity in Aircraft Plants: How Much Is DoD Paying? *(2002)*
- Reducing Defense Infrastructure Costs *(2000)*
- Strengthening Defense Resource Management in Emerging Democracies *(2004)*
- Synthetic Environments for National Security Estimates (SENSE) *(1998)*
- The Contingency Operations Support Tool (COST) *(1999)*

Force and Strategy Assessments

- Attack Operations against Critical Mobile Targets *(2000)*
- Confronting the Threat of Chemical and Biological Weapons: IDA's Chem/Bio Program *(1998)*
- Counterdrug Research *(1998)*
- Crisis Management Engagement Activities in Southeastern Europe *(2004)*
- Enlarging NATO: Opening Options for Aspiring Members *(2004)*
- IDA Studies of National Security Organizations and Management *(2000)*
- Quadrennial Defense Review Analysis *(2001)*
- Regional Implications of U.S. Policy Options for North Korea *(2004)*
- Taking the "Revolution in Military Affairs" Downtown: A DoD Roadmap for Improving Capabilities for Urban Operations *(2002)*
- The Psychology of Deterrence – A Quantitative Model *(2000)*

IDA
4850 MARK CENTER DRIVE
ALEXANDRIA, VA 22311-1882
TELEPHONE (703) 845-2000
INSTITUTE FOR DEFENSE ANALYSES