Making IT Happen

Transforming Military Information Technology

edited by Joseph N. Mait

Center for Technology and National Security Policy

National Defense University

September 2005

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense, or any other department or agency of the Federal Government. All information and sources for this paper were drawn from unclassified materials.

Defense & Technology Papers ***are published by the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.***

Contents

Preface

…what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge.
Sun Tzu, 300 BC

Information has always been critical to successful warfighting, as important as rapid maneuver, overwhelming firepower, and dependable logistics. The ever-increasing ease with which information can be accessed and transmitted has made information technology a cornerstone of military transformation. Common to each service is a de-emphasis on platforms, on the concentration of mass to provide overwhelming force, and an increased emphasis on networking to enhance warfighting capabilities.

Concepts for network-centric, as opposed to platform-centric, warfare borrow in large part from business models developed in the 1990s that use networks to empower staff. Replacing hierarchies strained by too many decisions with a network that puts staff directly in touch with individuals or information necessary to speed sales and product delivery provides a company with a competitive edge. The ability to lock out competitors by responding rapidly is an attractive feature of network-centric operations that is applicable to warfare.

Achieving network centricity requires the development of new tools and new technologies. However, although the Internet was developed by the Government and the Government provided considerable initial support for the electronics industry, it is the commercial market that has driven recent developments in both technologies. Indeed, not only do the demands of the domestic commercial market dwarf those of the U.S. military, the U.S. market is but one of many global telecommunications activities. Gone are the days when telecommunications was dominated by a single U.S. firm.

The democratization of information and information technology represents a significant challenge to the U.S. military's transformational goals. The military understands that it is only one customer in a large market, albeit a customer with a lot of clout. To meet its transformational goals, the military must engage the commercial market using new means and methods. At the same time the military must balance the attractiveness of commercial technology with requirements for security, reliability, sustainability, and, most important, interoperability with legacy technology.

With support provided by the U.S. Congress, the Center for Technology and National Security Policy at the National Defense University has investigated how the Department of Defense can enhance its engagement with the commercial market while meeting requirements for operations. For example, the Center has studied the attitudes of small information technology companies toward working with the government.[1] A chief complaint from this community is that they do not know what the services need.

[1] "Survey of Information Technology Firms," Schaefer Center for Public Policy, University of Baltimore, October 2003. Available at: <http://www.ndu.edu/ctnsp/IT Industry Survey.Uni-Baltimore Report.pdf>.

This work addresses that deficiency. This report is essentially a primer for commercial providers to gain some understanding of the military's thinking about military information technology and some of the programs it foresees for the future. Our intent is to introduce those not presently involved in the development of military information technology to some of the thinking and programs being developed by the Department of Defense for deployment in the next five to ten years. The report does not address research activities.

The organization and content of the primer requires some discussion. Information technology is the term used broadly by the Department of Defense to refer to the technologies, systems, and applications necessary to enable network-centric capabilities. However, the term conveys little of the breadth required. In preparing this primer we were aware that information technology for military operations can be parsed many different ways.

For example, the taxonomy used by the Office of the Secretary of Defense's Technology Area Reviews considers primarily technical applications, such as communications and networking, network assurance, modeling and simulation. But this list draws no distinction between hardware developed for the physical infrastructure and software developed for applications.

Alternatively, one can categorize information technologies according to their function. For example, there is a difference between the individual products, such as software programs (e.g., the human resources pay system for a service or an operations planning tool) and hardware (e.g., a network-based radio), and embedded technologies like the protocols that link a weapons system to a network, and between the infrastructure necessary to insure seamless and secure networked communications.

Yet another representation considers the nature of military operations. For example, infrastructure requirements differ if the operations occur at a sustaining base in the United States, versus in the field, air, and sea. Differences also exist if the operations are for logistics or combat. And, for combat, needs differ if the combat is air-, sea-, or ground-based, or combined, such as combined air-ground combat.

We present this discussion to make the point that any report on information technology must chose some means to look at the technology. We have chosen to take a diagonal cross section. That is, the report is organized primarily along service, joint, and coalition operations. However, each chapter provides a slightly different perspective on information technology.

The first three chapters summarize the thrusts of the Army, Navy, and Air Force programs in information technology. Although they share common themes, the programs reflect specific needs dictated by the operational environment of their service. The Army's program, in particular, is heavily influenced by its emphasis on the Future Combat Systems (FCS). Thus, although application integration is also important to the Army, we focus instead on the development of critical technologies required for tactical operations. Key among these is the development of mobile ad hoc networks and applications, especially command-and-control, that can be executed on them.

The discussion in chapter two emphasizes the technical objectives of the Navy's FORCEnet to meet its operational capabilities, characterized broadly as Sea Strike, Sea Shield, and Sea Basing. The chapter focuses on the functionalities that FORCEnet requires and the technologies to produce these functions. Further, the impact of systems and platforms on implementing FORCEnet are also discussed.

Chapter three provides a broad perspective of the Air Force's program. The chapter discusses activities in the Air Force Research Laboratory and the Air Force Battle Labs that support the Joint Battlespace Infosphere. This includes the operational capabilities Global Awareness, Global Information Enterprise, and Dynamic Planning and Execution, and some of the technologies required to realize these capabilities. The chapter further discusses how the Air Force integrates and tests these new capabilities in its battle labs.

Underlying the emphasis on information and networks is the desire for information sharing. Information technology enables increased situational awareness and improves the linkage between data collection assets and action officers. Data sharing implies not just coordination between, for example, surveillance assets and fire control systems, but also inter-service collaboration. Further, the increased likelihood for coalition fighting requires ad hoc means and methods to share information that do not leave a nation's forces vulnerable when coalitions change.

Technical and programmatic issues related to information sharing are addressed in Chapters four and five. Chapter four provides a detailed and complete overview of the issues and requirements necessary to insure networking and information sharing occurs across the services. The chapter characterizes the nature of the interoperability problem, describes recent initiatives to ameliorate interoperability shortfalls, and identifies interoperability challenges. In particular, the chapter emphasizes interoperability among systems in the context of joint, interagency, and multinational operations, including international organizations such the United Nations, nongovernmental organizations, and contractors.

The unique problem of sharing information with allies and changing coalitions is addressed in chapter five in the context of NATO operations. The chapter describes NATO’s efforts to move into an age of information-intensive military operations with particular attention on political decision-making, and the command and control of distant multinational operations. In this regard, the chapter focuses on the unique challenges faced by NATO and its member nations to field network-enabled military forces, including the Alliance’s command and control operating environment and technical architectures. These considerations affect the structure of NATO's information technology management organization and systems.

The survey of attitudes that prompted this report is only one of several projects on information technology conducted by the Center for Technology and National Security Policy. Other projects include cyber security and information assurance, the use of venture capital firms as a model for industrial outreach, the development of web-based tools as an adjunct to more personal methods for interaction between commercial providers and military users, and implications of the global nature of telecommunications on the U.S. and its military. Results from these projects and others can be found on the Center's website at: http://www.ndu.edu/ctnsp/information_tech.htm.

Chapter One

Information Technology for Army Tactical Needs

Joseph N. Mait
Richard Chait
Albert A. Sciarretta

1. Introduction

In a sustaining base, the military and commercial sectors share a common, often static, infrastructure of landlines, fiber optics, and wireless communications. Further, many military and commercial applications are similar, for example, business enterprise applications such as human resources. In such instances, even though security requirements may differ, the military can rely upon the commercial sector to offer solutions.

However, where commercial and military sectors differ most is in combat tactical operations, where the mobile infrastructure and applications together have no commercial equivalent. Although fire and rescue operations are similar in some respects to tactical military operations, domestic fire and rescue operations can rely upon a sustaining base infrastructure for communications. A tactical military operation must carry its network capabilities with it. Also, although logistics shares some requirements with its commercial equivalents, its requirement to supply warfighters implies adaptation of commercial practices and applications as opposed to simple adoption.

In this chapter we highlight the information needs unique to ground tactical operations. Further, we present the Army efforts within the overarching DOD framework to enhance data and information exchange among systems of systems on the battlefield. This emphasis on network centric operations and Army efforts to integrate command and control applications with logistics across all levels of command is discussed in Section 2. Section 3 discusses the technology required, including radios and network protocols, to provide these applications in a mobile situation. In Section 4, we look at some challenges facing the Army's Future Combat System (FCS) such as integrating technology and applications as exemplified by the Army's plans for a beyond-line-of-site networked fires capability. In Section 4 we also present other issues important to Army efforts to enhance information exchange on the battlefield. Summary comments are provided in Section 5.

2. Network Centric Operations

Vital to the transformation of U.S. military forces is the ability to conduct network centric warfare as defined in DOD Directive 8320.2[2] dated December 2, 2004 as "an information superiority- enabled concept of operations that generates increased combat power by networking

[2] DOD Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense", 2 December 2004.

sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization". This document also "directs the use of resources by the military departments to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG)," the defense-wide network architecture that enables data sharing for achieving net-centric warfare and operations. Other important policy directives and instructions, such as DOD Directive 4630.5[3] and 4630.8[4], establish policies and procedures, respectively, for the interoperability and supportability for all aspects of information technology (IT) and national security systems.

In line with the above guidance, the Army's overarching efforts to enhance its tactical network capabilities are focused on integrating its entire network capabilities from strategic to tactical and across all organizations and systems. This integration effort is critical to the Army's net-centric environment, known as LANDWARNET, and is the Army's portion of the GIG that will include all elements of the Army's communication architecture. The impetus for this effort is the removal of the stovepiped array of applications in the present Army Battle Command System (ABCS). The ABCS does not have adequate interoperability with the Army's tactical command and control (C2), the Force XXI Battle Command, Brigade and Below (FBCB2) application. Additionally, ABCS does not provide a strong link between C2 and assets for intelligence, surveillance, and reconnaissance (ISR), and runs independently of the Global Combat Service Support (GCSS) system. To support Army transformation, the vision is to evolve the Army's battle command information systems from the current state (Capability Block 1 with ABCS 6.4) to a desired state in 2016 (Capability Block 6 with the fielding of FCS and Joint Command and Control (JC2)).[5] Near term efforts will also include the integration of both combat command and combat service support. All efforts are focused on supporting future Units of Employment[6] and FCS-equipped Units of Action (a brigade size organization).

The backbone of the current Army system is the Warfighter Information Network-Tactical (WIN-T). The communications network over which voice, data, and video are transmitted consists of a varied array of channels. It will provide the connectivity for the FCS System of Systems Common Operating Environment (SOSCOE), which will support multiple mission-critical applications both independently and simultaneously. Currently, only the Single-Channel Ground and Airborne Radio System (SINCGARS), used to transmit voice and data, extends throughout the command structure from Corps to battalion. The Mobile Subscriber Equipment

[3] DOD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)", 5 May 2004.
[4] DOD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 30 June 2004.
[5] Battle Command Information System Integration & Migration Plan, Version 1.5, Coordinating Draft, 4 January 2005.
[6] A headquarters organization for multiple Units of Action. There are two levels of UEs: (1) UEx. A 1000-person war fighting headquarters that provides battle command of up to six BCTs or joint/coalition equivalents plus Support Brigades. At least one of each type Support Brigade will be attached to a UEx when it deploys. The UEx consists of command and control assets formerly associated with division and corps headquarters. (2) UEy. The Joint Forces Land Component Command headquarters in a theater of operations. It is capable of exercising administrative control of all subordinate UEx and theater support commands. It consists of assets formerly associated with corps and army headquarters.

(MSE) is available only from Corps to brigade and the Enhanced Position Location Reporting System (EPLRS), from division to battalion. Adding the Joint Tactical Radio System (JTRS) to the WIN-T will create a communication system that provides connectivity across all levels of command, as well as connectivity to the other services. The JTRS is a software based radio system currently being developed as the primary radio for providing communications to the military.[7]

The most visible application of networking to the battlefield is the FBCB2 system, presently deployed with the 4th Infantry Division and on all Stryker platforms. Through its capabilities in position-navigation and reporting, combat identification, and its interface to terrestrial communications, FBCB2 provides critical situation awareness information and command and control to the lowest tactical echelons. For operations over long distances or rugged terrain, there is also an interface to satellite communications.[8]

FBCB2 is also referred to as "blue force tracker" for its ability to track and display the movement of friendly forces, providing a real-time Joint Blue Force situational awareness for commanders, staff, and soldiers. It also provides a shared common picture of the battlespace, with the locations of friendly and enemy unit indicated on graphical displays.

Within a maneuver brigade, FBCB2 is a system of approximately 1,000 networked computers. The network is based on a fixed set of addresses, not a dynamic one capable of responding on its own to the conditions on the battlefield. Thus, prior to deployment, the network must be planned and addresses assigned, and, at a hardware level, frequencies and circuits assigned. Once operations have commenced, network resources must be constantly monitored and managed to reconfigure the network and deactivate circuits. That is, network reconfiguration and deactivation are not autonomous. The system is presently incapable of starting, operating, and gracefully degrading of its own accord under all conditions without human intervention.

The Army's present efforts in information technology are focused primarily on integration through the deployment of WIN-T and JTRS. The Army's future efforts are focused on Future Combat Systems, which includes distributed, collaborative planning and execution systems; self-configuring, mobile, integrated networks; extended non-line-of-sight operating ranges; and ISR assets available to the lowest tactical level. These capabilities are addressed in the next section.

3. Future Capabilities and Required Technologies for Army C4ISR

The operating dictum of the Future Force is to "see first, understand first, act first, and finish decisively." Whereas improvements in kinetic/non-kinetic effects and survivability are required to "finish decisively," achieving the first three objectives requires improved capabilities in command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).

[7] Widening the Net, U.S. Network-Centric Warfare, JDW, 26 January 2005, pages 24-29.
[8] Widening the Net, U.S. Network-Centric Warfare, JDW, 26 January 2005, pages 24-29.

Seeing first implies not only extending the range of sensors but also creating a network of the right mix of sensors to ensure constant and unwavering monitoring of an area. All sensors, from tactical to strategic, aerial to ground, and monitored to unattended, need to be integrated into the network. "Understanding first" requires the ability to fuse data from multiple databases and multiple sensors of varying types - including electromagnetic, radio frequency, and acoustic – with information from knowledge bases to detect, recognize, and identify threats and their intentions rapidly. "Acting first" implies rapid transmission about a threat and its anticipated actions to an appropriate responder. In an offensive operation this can be measured by the sensor-to-shooter time. Although peacekeeping may not require as severe a response, reducing the time between the detection of a threatening situation and a response to it can still save lives. Signal processing on-board sensor platforms, data compression, and decentralized communication are all capabilities that ensure rapid response. To ensure the response is appropriate, excluding human frailties, it is important for the network to be secure and robust to disruption.

These capabilities are tied intimately to the development of FCS. The FCS is a Joint network-centric system of systems, with separate functions for command and control, fires, transport, and sensing, distributed across relatively lightweight manned and unmanned ground vehicles, and unmanned aerial vehicles. The FCS systems will include the Warfighter, the network, and as many as 18 sensor, weapon, and logistics manned/unmanned systems.[9] The FCS is designed to enable Future Force capabilities, including the ability to fight immediately upon arrival into theater, to provide lethality through a networked sensor-to-shooter system, to provide organic capability for line-of-sight, beyond-line-of-sight, and non-line-of-sight fires; and to provide all-weather, all-terrain mobility and awareness over a large operating radius and area of influence.

The FCS systems will be linked to the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) network by a multilayered communications network with significantly improved mobility, security, range, capacity, and reliability. The network will provide integrated network management, information assurance, and information dissemination management of critical information both within and external to FCS-equipped organizations.[10]

The requirements for mobility dictate an untethered network, that is, a network without a fixed infrastructure. In a conventional network with a fixed infrastructure, servers, routers, and network devices have fixed locations and each device is tethered to the network through an Internet Protocol (IP) address. Moving a computer to a new location in a tethered network typically requires a new IP address and a visit from the IT service center to change the address on the computer. In an untethered network, all devices are mobile, including routers and servers. In battlefield environments, devices will be moving constantly on and off the network, which makes service visits from the IT HELP desk highly unlikely.

To ensure the stability of the network upon which many of the Future Force capabilities depend

[9] FCS 18+1+1 White Paper, "Overview of Future Combat Systems (FCS), Program Manager, Unit of Action," 15 October 2004. Available online at: <http://www.army.mil/fcs/resources/FCS%20White%20Paper.pdf>.
[10] FCS 18+1+1 White Paper, "Overview of Future Combat Systems (FCS), Program Manager, Unit of Action," 15 October 2004. Available online at: <http://www.army.mil/fcs/resources/FCS%20White%20Paper.pdf>.

requires the development of new networking technology and protocols. The network must be capable of self-organizing in an ad-hoc but energy-aware fashion. For example, unattended ground sensors must self-organize into networked clusters after deployment through airborne dispersal or hand emplacement. Re-establishment of the network may be performed periodically to ensure connectivity is not lost due to node destruction or failure. The network for mobile platforms, however, must be re-established constantly.

The remainder of this section covers in detail networked sensors, untethered communications, and protocols. This chapter will also look at FCS communications, command and control and their applications to NetFires.

3.1 Networked Sensors

To ensure the ability to see first in all situations, the Future Force must utilize ISR assets in multiple physical layers – ground, maneuver, high altitude atmospheric, and earth orbit. For example, because global surveillance assets have difficulty seeing through foliage or identifying threats in urban terrain, they must be augmented with tactical ISR assets in the maneuver and ground layers. This dictates the development of networked unattended ground sensors which can be emplaced remotely with artillery or air vehicles, as well as being placed on tactical unmanned aerial vehicles, on organic unmanned aerial vehicles, and on unmanned ground vehicles.

To ensure constant coverage over an area and to further ensure that no gaps exist in situational awareness, it is essential that these assets are distributed and networked, and be designed to operate in a power constrained environment under all weather conditions. Networking provides multiple views from different perspectives and different modalities, which enables cross-cueing among sensors. For example, acoustics sensors can be used as trip wires to wake-up imaging sensors. This example not only supports sensor fusion needs, but also provides a means for minimizing the use of power hungry imaging sensors.

Development of an efficient sensor network requires tools for sensor tasking, for data fusion, as well as small, lightweight, low cost, low power sensors. Uncooled infrared (IR) imaging sensors and directional acoustic sensors are currently the most mature technologies and represent the greatest potential for near-term impact. For example, when combined with visible imaging sensors, uncooled IR sensors can extend imaging capabilities from day into night. Such multi-spectral sensors can be mounted on unmanned ground vehicles, organic aerial vehicles, and unattended ground sensors.

However, initial studies indicate that the overall network is dominated by unprocessed sensor data, which impacts the architecture of the network. (Subsidiary to establishing a sensor network, robotic control of unmanned aerial and ground vehicles is also a major contributor to the network data load.) In a hub and spoke network, with sensors on the spokes and the C2 node at the hub, even though a bottleneck exits at the hub, the impact of the data is at least localized. In an ad-hoc network, the data may traverse several nodes before reaching the C2 node. Thus, the impact of unprocessed sensor data is felt throughout the network. On-sensor signal processing can be used to alleviate some of the congestion by performing data reduction and information extraction. Low power, high-speed radios and energy efficient networking protocols are also necessary.

3.2 Untethered Communications

Perhaps the most important distinction between a commercial wireless network and the Future Force network is that the subscriber and the infrastructure in the Future Force network are both mobile. The network is untethered. In a commercial wireless network a mobile subscriber is tethered to a fixed infrastructure. Infrastructure of the untethered network is constantly changing and must therefore be ad-hoc and self-organizing.

Although a subscriber connects to a commercial network in wireless fashion, all other connections are either wire or optical fiber. In an untethered network all connections are wireless. Thus, a constellation of fixed, hardwired towers is incompatible with an untethered network. The untethered network must rely solely upon on antenna technology to establish interconnectivity. For on-the-move operation, antennas must be small and have easily erectable masts, a low profile, or no profile, as is the case for conformal antennas, for example, antennas embedded in the surface of a platform. Ground operation imposes serious challenges on antenna and radio design, such as greater attenuation than in free space due to near-earth propagation. Low launch angles also limit antenna gain, as do multi-path, fading, and multi-access interference. An antenna should also have a low probability of detection and a low probability of intercept.

Further, the commercial network has greater frequency spectrum available to it than a military network. The assignment of frequencies to a military network is not only restricted but also impacted geographically. For example, frequency assignments in the U.S. are different than those in Europe. Additionally, the complexity is increased as future platforms with single antennas will be replaced with systems with multiple antennas, and narrowband radios will be replaced with multi-band communications systems. To ensure agility in the face of differing frequency assignments and multi-band communications, the JTRS will be a software-based radio.

Design of the communications network must consider the trade-offs between bandwidth, processing, system power, and system life. The tactical nature of the network also constrains it in energy and bandwidth. Thus, transmitters and receivers need to be energy efficient but must provide desired capability. The bottom line is to produce a system that can balance effectiveness against cost.

Consider, for example, that military transmissions must be difficult to detect, robust in the presence of jamming, and insensitive to interference. These requirements constitute an overhead on the available data rate: data headers and data redundancy are required to ensure security. However, high data rates are required to ensure low latency, e.g., small delays, between the detection of a threat and a response to it. Low latency is especially critical when targeting mobile and fleeting threats.

To meet the opposing constraints of low latency and security, DARPA's FCS-Communications Program uses a multi-tiered network. A low-band frequency compatible with JTRS is used for non-line-of-sight communications and a high-band (millimeter-wave) frequency is used for line-

of-sight communications. Both channels use directional antennas to ensure low probability of intercept and low probability of detection and spatial multiplexing of beam patterns to reduce interference between nodes.

There are many other related efforts for addressing the challenges of untethered communications, including the Army's numerous antennas and communications networking programs at the Communications-Electronics Research, Development, and Engineering Center (CERDEC) and DARPA programs, like the Networking in Extreme Environments (NETEX) program.

3.3 Protocols

Protocols are the data standards that computers use to ensure the proper transmission of and receipt of messages. A fixed infrastructure allows for protocols similar in function to those used by the postal service. Since streets and homes are immobile, house numbers and street names ensure proper delivery of the mail, rather than the name of the individual to whom the mail is addressed. With a mobile infrastructure, the name of the addressee is important and protocols for Mobile Ad-hoc Networking (MANET) need to be developed.

The objective of the Multifunctional On-the-Move Secure Adaptive Integrated Communications (MOSAIC) strategic technology objective is to demonstrate adaptive network protocols that are capable of supporting a mobile infrastructure. The goals of the program are to demonstrate an ad hoc network capable of self-organizing automatically, to demonstrate quality of service (QoS) protocols that allow multiple classes of traffic (e.g., voice, data, imagery) to share the same network resources, and to demonstrate network handoff between dissimilar networks such as between airborne and satellite nodes. These capabilities were demonstrated successfully in June 2004 at the Army's Mobility Assessment Test and Integration Center in New Mexico. The protocols were tested in tactical ground-to-ground and ground-to-air links, as well as commercial wireless local area networks and military satellite links. Inclusion of these latter links demonstrated the protocol's ability to interoperate with commercial routers and legacy defense communication equipment.

Given that the network is critical to survivability, the amount of latency, or delay, is a critical parameter and reconfiguring the network manually robs operations of precious time. Thus, the conditions faced by mobile ground forces dictate an ad hoc network. That is, the network must be capable of reconfiguring itself constantly as nodes come onto or fall off of the network. Unfortunately, the MANET protocols necessary to sustain the network reliably remain under development and the Internet Engineering Task Force, the protocol engineering and development arm of the Internet, has not yet accepted any standards.

3.4 Radios

The utility of mobile ad hoc networking has already been demonstrated in DARPA's Small Unit Operations Situational Awareness System (SUO SAS) and in DARPA FCS Communications. SUO SAS is a MANET-based networked radio designed for a unit cell of 20 dismounted soldiers. It was successfully demonstrated in a simulated helicopter rescue at Ft. Benning in October 2002 and has since been transitioned to the U.S. Army Communications-Electronics

Command (CECOM) for further development and evaluation at larger scale experiments. In August 2003, FCS Communications demonstrated a MANET-based networked radio system for a unit cell of 20 ground vehicles and two aerial vehicles in a mock operation at the Army National Guard Orchard Training Area in Boise, Idaho. FCS Communications demonstrated 10 megabytes per second data rates with latency on the order of 100 milliseconds. This performance is needed to support real-time fire control and robotic missions yet provide robustness to jamming and low probability of detection. FCS Communications uses both directional antennas at low frequency bands, which match frequencies allocated for the JTRS, and directional antennas at millimeter-wave frequencies.

DARPA's efforts demonstrate the maturity of the communications technology that forms the infrastructure of the Future Force network but by itself does not provide any operational capability. Operational capability is provided by the applications executed over the network. This capability has yet to be demonstrated, but is currently under development. Mobile command and control is the focus of the Agile Commander Advanced Technology Demonstration (ATD) under the direction of the Army's CECOM and DARPA's FCS Command and Control program.

3.5 Command and Control Systems

The sensors, antennas, computers, protocols, and radios alone do not address all of the needs for an Army battlefield information system. There is a need for Battle Command (BC), vis-à-vis command and control (C2), applications. Rapid Army fielding of advanced systems like DARPA’s Command Post of the Future (CPoF) in Iraq have shown how such BC systems can truly be force multipliers and support force protection. The Army’s past recognition for the value of BC systems prompted it to initiate programs such as Agile Commander, C3 on the Move, C2 in Complex and Urban Terrain, and many similar efforts. DARPA also continues to commit resources to advance BC systems, like the Integrated Battle Command program, which will provide more agility for pulling together various components of an IT network. FCS BC will benefit greatly from each of these efforts.

4. Some Challenges

4.1 FCS Command, Control, Communications as Applied to NetFires

The complexity of the FCS as a system of systems implies that Future Force capabilities cannot be achieved simply through maturing technologies. Rather, they are dependent upon integrating heterogeneous systems that have various levels of maturity. For example, the capacity for beyond-line-of-sight fires embodied in the Future Force vision requires a sensor network linked through a mobile network to a C2 node, which is in turn linked through a mobile network to a weapons system.

A discussion of DARPA's NetFires program provides insights into the issues related to integration. NetFires is a containerized, platform-independent, multi-missile package capable of engaging targets between 25 and 50 km away, as well as a soft-launched loitering attack missile capable of hitting targets between 40 and 100 km away. The loitering attack missile can remain above a designated area for up to one hour before engagement to collect data for situation

awareness. Although the mechanical operation of the missiles has been demonstrated, this alone does not provide a beyond-line-of-sight fires capability.

Critical to the mission success of NetFires is the demonstration of its C2. The goal of DARPA's FCS C2 program is to create a prototype application for a network of manned and unmanned systems and validate a new approach to battle command. The intent is to push as much of the data integration as possible to the sensors to free commanders and battlespace managers of the integration burden so they can respond more accurately and rapidly than presently.

Original requirements for C2 were relatively simple and included, for example, target location updates to missiles with position and status information, small target images, and a link to a forward observer. However, program evolution and user desires have increased the complexity of the system to include control of a large numbers of missiles, missile-to-missile coordination, provisions for continuous imagery from a seeker, and relays to extend the ranges of the missiles.

The operational concept for NetFires dictates separate command, control, and communications (C3) needs for its air and ground elements. Interoperability with legacy systems is critical for the ground segment. Ground communications must be designed to operate with current assets, e.g., SINCGARS and EPLRS radios, but also need to accommodate MOSAIC and FCS Communications when they become available. C2 for the ground segment must operate with legacy applications such as the Advanced Field Artillery Tactical Data System (AFATDS) and FBCB2, but need to add a real-time mission manager and a communication system controller.

The ground element of the C2 application must perform several functions. The application must perform mission planning, including specifying waypoints over terrain, determining mission type, and setting target priorities. As part of mission execution, the application must provide target nominations, show missile status, and coordinate a group of missiles to ensure mission completion and airspace deconfliction. The application must also serve as a communications manager by allocating frequencies and bandwidths to communication links and displaying the status (e.g. data rates) of links. Critical to its role as communications manager, the application must be able to provide graceful degradation of the network during communication outages.

The operational concept for NetFires imposes stringent requirements on the air segment C3. For example, the system must be able to respond automatically to changes in air segment communications. Under normal conditions, the system should provide forward communications to the missile for guidance and control while simultaneously receiving target imagery from it. If communication is lost completely, the system must have some level of autonomous capability. With degraded communications, missile control remains critical but the receipt of target imagery can be abandoned.

To control a large numbers of missiles, a two-tier architecture has been proposed. A single missile, designated as a group controller missile, uses two simultaneous communications channels selected in accordance with the proposed FCS Communications architecture. One channel communicates with up to 14 subordinate missiles and a forward observer, while the second channel is used to communicate with the C2 node.

Since one of the goals of the C2 program is to perform target integration as close to the sensors as possible, the controller missile uses target range and its priority to set the format of the target imagery and its data rate for communication with the C2 node. Since the controller missile is used as a gateway to the C2 node, it must have the ability to manage target imagery, including the management and correlation of images from its subordinate missiles and other ISR assets.

As stated in the beginning of this section, realization of a beyond-line-of-sight fires capability requires the integration of multiple technologies. At the present time, mobile ad-hoc communication between 20 mobile ground nodes and a single aerial node have been demonstrated in two field tests at Lakehurst Naval Air Station, New Jersey and a third at the National Guard Training Center in Boise, Idaho. As part of the third demonstration the ABCS C2 application will be executed over the network. The FCS C2 remains under development at the U.S. Army CECOM at Ft. Monmouth, New Jersey. Demonstrated capabilities include target imagery manipulation and hand-off to a forward observer, but the advanced capabilities in mission planning and execution, and in communications management have not yet demonstrated, let alone executed over an ad-hoc network consisting of 15 aerial nodes.

4.2 Other FCS Challenges

The FCS communications network will be comprised of several homogeneous communications systems such as the JTRS with Wideband Network Waveform (WNW) and Soldier Radio Waveform (SRW), Network Data Link, and WIN-T. FCS will need to leverage all available resources to provide a robust, survivable, scalable, and reliable heterogeneous communications network that seamlessly integrates all systems of systems components. Further, realization of new capabilities will be aided if development leverages trends in industry. In the discussion below we highlight some of the difficulties engendered in both these requirements.

With regard to protocols, the long-term focus of Army efforts are on MANET protocols. However, commercial industry is moving toward an all-IP core network for its 4th Generation wireless networks. An all-IP network would allow the military to leverage commercial developments in applications, network management, routing, and security tools, and would allow the military to provide a common basis for interoperability. However, IP provides limited support for quality of service protocols in real-time (especially latency), poor mobility and hand-off, low overhead efficiency, and poor quality voice transmission. Even more critical to defense operations, an all-IP network provides a common basis for any cyber or information operations attack. Although IP version 6 accounts for mobility of the user from computer to computer, it does not provide for mobility of a node.

At the physical layer, a significant near-term synchronization of JTRS and WIN-T with FCS is required. According to present documentation, WIN-T is expected to support communication between tactical operation centers (TOCs), which are transportable but not necessarily mobile, using the JTRS wideband networking waveform. Data rates for TOC-to-TOC communication are required to be 5 Megabytes per second (Mbps). WIN-T is also expected to support communication between a mobile node and a TOC.

However, overhead assets will be a critical part of the FCS network: terrestrial line-of-sight

communications alone is insufficient to meet network needs. Mobile Ad-hoc Networking for the Future Force is expected to support data rates between 10 and 120 Mbps for communication between ground mobile nodes and between ground mobile and aerial nodes.

The difference in data rates and links raises several questions. For example, with what data rate can WIN-T support mobile battle command, e.g., C2 on-the-move, over terrestrial, airborne, and satellite links? Can the wideband networking waveform provide legacy TOC-to-TOC connectivity and FCS Mobile Ad-hoc Networking in the same waveform? Can wideband networking waveform be used for both FCS ground-to-ground and FCS ground-to-aerial links? How do the communications links required for mobile battle command compare to those required for FCS? Further, the current and planned military satellite communications terminal population does not appear to match FCS requirements and needs.

4.4 Interoperability

In order for FCS BC to operate as an efficient, effective system of systems, a significant amount of effort must be placed on interoperability. Joint Publication 1-02[11] defines interoperability as "The ability of systems, units or forces to provide services to accept services from other systems, units or forces, and to use the services to enable them to operate effectively." However, as Zavin[12] has stated: "Interoperability is more than just the technical exchange of information: it impacts systems, process, procedures, organization and missions over the life cycle; and it must be balanced with Information Assurance." A critical challenge for Future Force information systems will be to achieve interoperability among Army BC systems, as well as with all joint, coalition, and non-government systems. The challenges of interoperability are discussed in another chapter of this book.

4.5 Modeling and Simulation

For FCS there is a need to evaluate large-scale communications and sensor networks of networks to examine issues of scale, performance predictions, and validation of theoretical models for large networks. Modeling and simulation (M&S) is an indispensable tool for studying the behavior of communications and sensor networks. Current communications network models and simulations examine up to a few thousand nodes, while sensor networks may be much smaller. Additionally, current propagation and performance models account for digitized terrain, natural features, and weather effects; but they are severely limited by manmade feature data, especially urban structures. To support the development of FCS information systems, there is a need to develop computationally efficient models of large scale communications and sensor networks which take into account the physics-based characteristics (e.g., multi-spectral emissions) and constraints (e.g., impedance to RF propagation) of natural and man-made (especially urban) environments. FCS commanders will need to use these same simulations, in real time, to support operational communications and sensor network deployment and management.

[11] Joint Publication 1-02

[12] Jack Zavin, "Net-Centricity & Net-Ready – Beyond Technical Interoperability and C4ISR," Chief, Information Interoperability, DOD CIO/A&I Directorate.

6. Summary

The strategic advantage of the Future Force over its adversaries depends upon information superiority gained through FCS's mobile, networked, self-configuring C4ISR systems. Reducing latency among BC systems, weapons, and ISR assets should allow the Future Force to detect, track, and engage mobile and fleeting targets. Realizing these capabilities though requires an investment not only in individual technologies such as low power software-based radios (also known as JTRS) but also in the integration of many diverse information technologies (sensors, antennas, computers, protocols, and M&S). Currently, the Army's greatest unmet needs are in the development of MANET protocols and architectures; collaborative BC applications that can be executed over a distributed network; the fusion of data from self-configuring, networked sensors; interoperability; and computationally efficient models and simulations of large scale, realistic communications and sensor networks.

Chapter Two

Naval Information Technology

Elihu Zimet

1. Introduction

The operational concept of Network Centric Warfare (NCW) has its roots in the Navy. The Navy viewed the explosion in information technology (IT) as a gateway to integrate its geographically dispersed forces and as a means to enhance response time and agility. This is reflected in the Navy and Marine Corps strategy for transformation, Sea Power 21. Under Sea Power 21 naval air, surface, underwater and space elements form a unified force that projects offensive power and defensive capability.[13],[14] The offensive and defensive capabilities are encompassed in three operational capabilities: Sea Strike, Sea Shield, and Sea Basing. Critical to their realization is FORCEnet, the information infrastructure that integrates sensors, networks, decision aids, weapons, humans, and supporting systems into a comprehensive system.

Due to the inherent separation and isolation of Navy ships and submarines, and the expeditionary mission of the Marine Corps, NCW represents a real "sea change" for traditional naval operations. Consider that until satellite communications became routine, communication between ships was limited to line-of-sight. Thus, surface ship task groups, which operate well beyond each other's line-of-sight, had developed a culture of independent latitude. Due to a submarine's dependence upon stealth for its survivability, submarine communications were even more limited.

Now, however, naval forces hope to counter current and future threats through effective command and control across Navy task forces and in conjunction with the other services. This requires strengthening current information and "knowledge superiority," that is, the ability to acquire and use knowledge of the battlespace to operate faster and more effectively than the enemy. Networking technology allows for collaborative and rapid planning, reduced target detection and acquisition times, reduced decision times, and increased precision and lethality with a reduced number of warheads.

[13] T*he Naval Transformation Roadmap,* Available online at: <http://www.dtic.mil/jointvision/naval_trans_roadmap.pdf>. [accessed 17 September 2004].
[14] Vern Clark, "Sea Power 21: Projecting Decisive Joint Capabilities," *United States Naval Institute Proceedings,* vol. 128 no. 10, pg. 32 (October 2002). Available online at: <http://www.chinfo.navy.mil/navpalib/cno/proceedings.html>. [accessed 24 September 2004].

Transformational capabilities for naval forces enabled by IT include the following:

- *Persistent Intelligence, Surveillance, and Reconnaissance (ISR),* in conjunction with networked joint and national capabilities, provide prompt and precise battlespace awareness any time and in any weather.
- *Time Sensitive Strike* brings precise, lethal effects to bear in decisive quantity on operationally significant targets within minutes and, ultimately, within seconds of target detection.
- *Ship-to-Objective Maneuver* projects a combined arms force from ships at sea directly against operational objectives, some located far inland.
- *Theater Air and Missile Defense* projects a protective and highly effective umbrella over the horizon at sea or deep inland, and from ground level to the exosphere, against all forms of aircraft and ballistic or cruise missile threats.
- *Littoral Sea Control* for control of the seas near land, assures prompt access and freedom of maneuver by sea-based joint forces confronted by surface and air threats quiet submarines, and mines.

These capabilities have become crucial to the services in the current global security environment and represent the direction of naval transformation. In this chapter we discuss the Navy's Information Technology efforts to achieve the goals of FORCEnet. Prior to a description of the technology the chapter will cover a brief overview of the operational environment in which it must operate its global information network. This is followed by a brief description of the operational processes and functionality that are inherent in the operational cycle of detecting targets, deciding on a course of action, and commanding and controlling platforms and weapons. A description follows of the component level of systems (e.g. platforms, weapons, sensors, communications, and computers of platform and systems) that form the pieces of the FORCEnet architecture.

2. Naval Operational Environment

The naval enterprise is globally dispersed at sea and on land, and operates from the ocean floor to the ocean surface and from the ocean surface to space. Naval Forces utilize seabed sensors, submarines, sea and land vehicles, as well as Navy and Marine Corps aviation and space assets. The scale of naval systems ranges from equipment for the dismounted marine to the largest naval vessel, the aircraft carrier. The complexity of tying these systems, platforms, and components into a networked cohesive force implies that FORCEnet is not a system, or even a program, but rather a framework for integration and alignment that will evolve as technologies allow. In addition, the FORCEnet architecture must be compliant with the overall DOD network architecture, which requires common standards and protocols.

The global dispersion of naval assets, the range of environments (underwater, air, and space) and the multiplicity of its systems frame the architecture for FORCEnet. In general, naval assets are situated beyond communications line-of-sight of each other and at sea have limited access to communication nodes other than satellites. Submerged submarines have unique communications requirements both because of their underwater environment and their requirement to remain covert. Surface ships also require signature and emission control and, although an aircraft carrier

is the largest platform in the military inventory, even it is limited in topside real estate for antennas. At the other extreme in scale, the dismounted Marine at the edge of combat operations needs to be networked into the support structure at sea and in the air.

3. FORCEnet Operational Processes and Functionality

FORCEnet will be the naval forces extension and implementation of joint architectural constructs, in particular, the Global Information Grid (GIG).[15] The GIG will be DOD's deployment of an information infrastructure and will provide a set of secure information and telecommunication services that will enhance decision-making and collaboration. The GIG will include multimode data transport media including landline, radio, and space-based elements integrated into an internet that dynamically routes information from sources to destinations in a manner transparent to the user.

FORCEnet is not a specific program or set of systems. Instead it is an operational and architectural framework that integrates people and systems into a networked, distributed combat force, and that scales across all levels of conflict from seabed to space, and sea to land.[16] Objectives of FORCEnet include:

- Providing information for the warfighter: FORCEnet will turn data into information that can be easily accessed and understood by the warfighter whenever and wherever the warfighter needs it.
- Providing consistent and integrated pictures: FORCEnet will provide an integrated tactical, operational, and strategic picture that accurately reflects the battlespace, and crosses the bounds of other U.S. armed services, agencies, allies, and coalition partners.
- Providing information to everyone, everywhere: FORCEnet will provide information to everyone — from central command to the warfighter at the edge in all operating environments.
- Providing predictive battlespace awareness: FORCEnet will enable the warfighter to anticipate the future battlespace, and support improved alternatives analysis and enhanced battle management.
- Teaching and training decentralized execution and self-synchronization: FORCEnet will advance warfighting proficiency in independent task level execution based on overall operational synchronization in the battlespace.
- Developing survivable and redundant networks: FORCEnet will employ a highly reliable and secure information infrastructure that will adapt to the warfighter's needs in all operating environments.

Ultimately, the purpose of FORCEnet is to provide the framework for military operations. The elements of a military operation, such as attacking a target, are detection, information processing

[15] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC, CCRP, June 2003), 186-198.
[16] *Chief of Naval Operations Strategic Studies Group XXI*, (Providence: Naval War College, July 2001).

and decision-making, followed by action (this is a cyclical process sometimes referred to as the OODA loop which stands for Observe, Orient, Decide and Act). The Navy breaks these elements into three components: situation awareness and understanding; planning and force management; and direction, action, synchronization and control. Situation awareness and understanding can be achieved if all elements of the force receive information tailored to their needs. Planning and force management is necessary to develop courses of action for all warfighting and support functions. Coordination of intended actions and any deconfliction are performed force-wide at this stage. Replanning is a continuous process that continues even during mission execution. Connectivity must therefore be maintained to ensure synchronization, direction and control between naval forces and other elements of the force.

A network-centric approach to minimize the cycle time of the OODA loop requires reliable and assured connectivity, the management and dissemination of information, as well as its processing and assessment. Maintaining connectivity and providing network service management among globally dispersed entities from capital ships to mobile users ashore is perhaps the most critical function to enable NCW. Connectivity must be maintained dynamically as systems move in and out of the network, yet this function must remain as transparent to a user as it is in a cellular telephone network. Connectivity must be continuous, with no interruptions in service, and have sufficient bandwidth to handle the flow of information. In addition, the integrity of the information must be maintained across the entire network.

But connectivity alone cannot achieve a commander’s intent. This requires rapid decision-making, which is dependent upon the management and dissemination of information. Providing time critical information to those in need is paramount, especially "disadvantaged users," like mobile ground units, whose capabilities for reception, processing, and display may be limited. Processing and display are critical technologies for turning raw sensor and intelligence data into formatted information that is easily understood and conducive for taking action.

4. Component Level of Platforms and Systems

The architectural and operational frameworks that define FORCEnet must ultimately be realized by and incorporated into all types of platforms. The advent of weapons that incorporate guidance, sensors, on-board processing, and data links has diminished the distinction between platforms (such as aircraft) and weapons (such as missiles). Thus, from the perspective of information gathering and information distribution, weapons are now part of the network. Platforms that incorporate the network thus range from large weapons carriers to individual munitions and from large sensor carriers to individual sensors. However, since the human remains the central node in FORCEnet for information management, decision-making, and information dissemination, system-level elements for command and control are essential.

Platforms house the network. Platforms may also be part of the sensor network and, simultaneously, a carrier of weapons. Within the NCW paradigm, platforms should be distributed, rapidly deployable, and reconfigurable for multi-mission capability. Between the Navy and Marine Corps, naval forces utilize every type of platform available to the military.

Two platforms unique to naval forces, the large surface combatant ship and the submarine, present unique challenges for networking. On a large combatant ship the large number of high power emitters for communications, navigation, surveillance, targeting, and electronic warfare create special interference problems for network management. (There are currently over one hundred emitters on an aircraft carrier.) For new submarine missions in the littorals it is imperative to link submarines into a tactical network, however both underwater acoustic and laser communication present unique challenges in terms of bandwidth and availability of service.

Sensors: Highly distributed, persistent and, often, autonomous sensors provide the surveillance required to produce a common operating picture essential to NCW. However, no single generic sensor exists. Sensors consist of a great many different devices designed to measure a broad number of signatures for different applications. To create a common operational picture it is necessary to fuse information from multiple sensor types.

In the electromagnetic spectrum, for example, sensors measure ultraviolet signatures from propellants for gun fires and missile launch; optical signatures for imaging and targeting; infrared signatures for night vision, thermal detection and targeting; short wavelength RF (millimeter wave) is used for imaging and precision targeting; mid-wavelength RF is the principal radar surveillance and targeting asset; long wavelength RF is used for over-the-horizon transmission for early warning and for foliage, earth and structure penetration. Sensors to detect and measure signatures other than electromagnetic are also being developed including acoustic sensors in the air, ground (seismic sensors) and underwater. Sensors can also be used to measure chemicals in the environment or radiation levels from radioactive particles. Sensors can be passive, i.e., they simply measure the emissions given off by a target (most IR seekers are passive) or active. Active systems typically illuminate a target to enhance information in the returned signal. Targeting radars, for example, are active systems.

Command and control (C2) provides the overall force and battle management to the networked forces to carry out the commander's intent. Inherent in command and control is the ability to gather and interpret information about rapidly changing situations to make decisions and issue orders. This requires the ability to process, assess, and share information. Despite the desire for "accurate information," what is ultimately presented to a commander may be incomplete or inconsistent. Automated software C2 aids must be able to fuse information and draw inference from disparate sources. Software to create a virtual collaborative working environment is also necessary.

5. Naval Technology for NCW

Although NCW incorporates platforms, weapons, sensors, and people, the backbone of NCW is connectivity and distributed decision-making enabled by information technology. The Navy and Marine Corps have an ongoing technology development and demonstration program to reduce technical risk and to demonstrate deployable prototypes for the FORCEnet concept.[17] The naval science and technology program consists of two elements: *Engineering and Deployment,* and *Discovery and Invention.* Engineering and Deployment provides the advanced development and

[17] Bobby Junker, "A Roadmap for the Navy ForceNet Program," presented at the Military & Aerospace Electronics East 2004 Show, May 18-19, 2004, Baltimore, MD.

demonstrations necessary to provide military relevant systems to the operational Navy and Marine Corps, whereas Discovery and Invention develops the fundamental science and exploratory development that forms the foundation of the technology base.

The Engineering and Deployment program includes a completed Advanced Concept Technology Demonstrations (ACTD) in IT (Extending the Littoral Battlespace) the JTF WARNET effort, and an IT-related Future Naval Capability (FNC) program (Knowledge Superiority and Assurance). The FNC has produced several accomplishments described below and has been restructured into a new FNC appropriately named FORCEnet. The naval FNCs are significant technology programs with brokered transitions to acquisition programs.

Extending the Littoral Battlespace (ELB), completed in 2001, was an ACTD dealing with NCW. The program demonstrated the ability to network ships at sea to tactical units ashore using airborne relay assets for beyond line of sight communication. ELB successfully demonstrated the concept of dynamic networking and provided operational forces with networked radios after the demonstration was completed but it did not demonstrate many of the attributes required for a fieldable system, such as, information integrity and reliability.

JTF WARNET, a follow-on effort to ELB, completed a deployable prototype in September of 2003 that will continue to demonstrate capability through 2011. JTF WARNET provides tactical connectivity using existing communications systems and a surrogate for the Joint Tactical Radio System (JTRS). The thrust of the program is to enable joint warfighting. This includes the ability to provide data for a common tactical picture, to integrate service fires and maneuver, and to demonstrate networked collaboration. Tools for system management of the network and applications have been fielded with the prototype, including the ability to map node locations and display connectivity. The effort continues to evolve including the addition of Tactical SATCOM to enable “communications on the move” between Navy, Marine Corps and Army units. However, JTF WARNET will not solve all technical issues associated with tactical networking, such as dynamic network reconfiguration to allow new sensors and information sources to be integrated into the network in a manner transparent to the user. JTF WARNET also does not address multi-level security and the human-machine interface (human comprehension of complex information).

The next supportive level of naval IT technology development was the Knowledge, Superiority and Assurance (KSA) FNC, which addressed five “enabling capabilities”: Common Consistent Knowledge; Dynamically Managed, Interoperable, High-Capacity Connectivity; Time-Sensitive Decision making; Distributed Collaborative Planning and Execution; and Enterprise-Wide Integrated Information. To achieve these capabilities, the KSA FNC consisted of several technology programs, each focused on transition to an acquisition program. Five projects are highlighted here that have developed technology being incorporated into development programs. These projects address data links, data management, communications, decision aids, and antennas.

Link-16 is a dedicated data link used jointly by the services to transmit information between platforms and munitions. For example, Link-16 can be used to exchange targeting data between aircraft and ships, and between platforms and missiles. The KSA FNC has provided Link-16

with dynamic networking capabilities. This was achieved by allocating communication time-slots dynamically, which improved the flexibility, throughput, and latency between sensor and shooter in Link-16. With the addition of a dynamic networking capability Link-16 can be used more broadly in establishing a mobile wireless network than just as serving as a targeting link including data and voice transmission.

A second program, the eXtensible Tactical C4I Framework (XTCF), addressed constraints on command and control due to the inability to exploit information from new sensors rapidly, the limited level of fusion from different input sources, and the limited amount of intelligence and track type data that is available to the network. The objective of XTCF was to develop a data management framework and tactical management system capable of supporting a wide range of mission applications, and also capable of permitting a seamless and rapid integration of information, and surveillance and reconnaissance data into a common picture. The program has transitioned to the FORCEnet Infrastructure.

To maintain an ad hoc network over a large tactical area requires some means for over-the-horizon communications using line-of-sight radios. The third KSA FNC program, Naval Battleforce Network: Airborne Communications Package, will provide a lightweight, multi-beam, wideband, multi-frequency antenna for an airborne relay to provide over-the-horizon connectivity for Link-16 data transmission and for networking radios such as JTRS. The antenna will be field tested in the Fall of 2005.

The fourth program seeks to reduce from hours to minutes the time required to coordinate multiple carrier strike aircraft against emergent targets. Decision aids developed under the Realtime Execution and Decision Support (REDS) program provide dynamic asset reallocation with weapon-target pairing, route assignment, and route validation. It also provides a knowledge-based monitor of the current operational environment and real-time force risk assessment for pop-up threats as well as targets. The program is currently supporting the Global Hawk UAV program.

The fifth KSA FNC program, Advanced Multifunction RF antenna (AMRF), addresses the problem of the increasing demands for additional antennas on platforms and the related problems of resource allocation and interference. AMRF seeks to overcome this problem by combining the antenna functions of radar, electronic warfare, and communications into a single wide-band shared aperture. An S-band antenna developed with this technology addresses Theater Ballistic Missile Defense.

The new Future Naval Capability (FNC) program at ONR, FORCEnet, has been structured into three major capability areas that are structured to provide transitionable products and are described as follows:

- Rapid, Accurate Decision-Making
    - Joint architectures for rapid, interoperable sharing of mission relevant sensor data and joint command and control
    - Automated image understanding and presentation of complex information for aiding in intent as well as situation awareness

    - Automated integration of disparate sensors and sources of information including metadata
    - Automated Courses of Action under uncertainty and risk including urban warfare
- Mission-Focused Communications and Networks
    - Dynamic, mobile networking of Navy and Marine Corps distributed operations where COTS fails
    - Automated dynamic spectrum assignment and dynamic resource and frequency allocation
    - Networking with directional antenna systems among airborne, ground nodes, surface and sub-surface
    - Open standards based secure digital voice capability for end-to-end interoperability between tactical users and users with high speed connectivity to the GIG
    - Mobile ad-hoc undersea acoustic or optical frequency communication among undersea sensor networks and undersea platforms including multi-path algorithms to improve link margin
- Pervasive and Persistent Sensing
    - Autonomous and dynamically reconfigurable tactical small UAV sensor networks including high resolution visible camera, Near IR and Long Wave IR cameras, active/passive Millimeter Wave imager, 3D monostatic/bistatic Synthetic Aperture Radar and GPS with a Swarm View control and ground station
    - Automated processing at the sensor and sensor networks
    - Automated self-control and self-tasking of sensors and sensor networks
    - Jam-resistant GPS and Non-GPS navigation

To address emerging opportunities and future threats, the Navy and Marine Corps maintain a basic research and applied science program called *Discovery and Invention*. The naval research program is coordinated with other service programs and is performed in universities, government laboratories, and industry. The twenty-eight technology areas listed below highlight the priorities of the naval IT Discovery and Invention program. The technologies are grouped within nine functional headings.

- Universal, Seamless, and Robust Communications, Connectivity and Network Service Management
    - Data Transport and Transmission Systems/ Data Links
    - Networking, Switching and Routing
    - Network, Communications and Computational Resource Management
- Information Distribution Management
    - Interoperability Software
    - Information Access and Delivery Software
    - Computer-Aided Reasoning
    - Fusion of Information into Knowledge
- Distributed Computing Infrastructure
    - Electronic Devices and Components
    - Network Computing Services
    - Power Sources

- Situational Understanding and Visualization
    - Information Integration Software
    - Computer Aided Reasoning
    - Estimation and Inference Engines
- Cooperative/Collaborative Processing Technology
    - Cooperative Software Agents
    - Optimization Software for Quality of Service
    - Collaborative Environment
- Human-Machine Interface
    - Situational Awareness and Visualization
    - Natural Language and Foreign Language Interface
    - Computer Aided Reasoning
- Information Security Technology
    - Security Software and Protocols
    - Positive User Identification
    - Adaptive Information Access
    - Intrusion Detection and Response to Attacks
- Assured Information Integrity Technology
    - Encryption Devices
    - Biometrics, Smart Cards, Digital Signature
- Modeling and Simulation for Situational Analysis and Information Management
    - Algorithms and Processes
    - Automated Learning
    - Distributed Intelligent Agents

Several initiatives in the Discovery and Invention program, described below, complete this discussion of the naval IT program. These initiatives are longer term in nature and are at an earlier stage of development.

Nanoscale electronics for distributed processing and high-density data storage

Many of the Navy's future operational capabilities require distributed computation to reduce overall communication data transmission and small, distributed nodes with a high level of computational capability, for example, small UAVs in a sensor network. To realize increased computational ability without a concomitant increase in size and weight dictates an increase in the chip logic density. Nanoelectronics is the technology concerned with reducing the feature size of logic elements (switches like transistors) to 20 nanometers (nm) or less, which is necessary to achieve an increase in density. Current feature sizes are less that 200 nm. Although at least two more generations of chips are planned, scaling the current silicon technology, the metal-oxide semiconductor, field-effect transistor (MOS-FET) any smaller is limited by quantum tunneling and energy density problems.[18] New technologies therefore need to be investigated. Promising, but still immature, technologies capable of potentially increasing logic density

[18] Gerald M. Borsuk and Timothy Coffey, "Moore's Law: A Department of Defense Perspective," *Defense Horizons* 30, (Washington, DC: National Defense University Press, July 2003).

include carbon nanotubes, quantum dots, magnetic semiconductor materials, and even biological materials.

Underwater acoustic networks

Information can be transmitted through the ocean either electromagnetically or acoustically, but both have significant limitations. For example, due to absorption and scattering, electromagnetic radiation does not propagate well in water. Although significant efforts have been made since the early 1980s to develop high power blue-green lasers capable of communicating from space with submerged submarines, significant technical and engineering issues remain and the communication is only one-way.

In contrast, sound travels well through water but acoustic transmissions have limited bandwidth. To overcome this limitation, it is possible to operate an underwater acoustic network in a fashion analogous to a cellular phone network wherein the cellular phone link to a transmission tower is replaced by an acoustic link from an underwater vehicle to an underwater acoustic modem. The modem can then transmit through a surface antenna to other modems and to other elements of the network above the surface.

An underwater network coupled to other elements of FORCEnet would utilize not only the submarine in new roles such as a strike platform in the littorals but also other underwater assets such as Unmanned Underwater Vehicles for shallow water mine detection and clearance.

Integration and presentation of dissimilar information

A number of technologies are required to process the vast amounts of data currently available through a network into useful information that can be assimilated and used by a decision maker or warfighter. Information overload can become a significant problem, particularly when decision times are short and the decision maker is under stress. The objective is to provide actionable knowledge with insight into uncertainty and risk as well as the nature of the source, the timeliness, quality and rate of degradation of the information. Three technologies associated with this objective are described.

Information for the warfighter is produced by dissimilar systems in dissimilar formats at different times and at different rates. A particular problem is to automatically overlay imagery to provide a comprehensive mosaic in which multiple frames are seamlessly stitched together without an operator to select tie points. Software is being developed to provide a registered global view automatically for targeting and for a common operational picture.

A second technology deals with the automation of image understanding. Significant problems exist in combat identification resulting in “friendly” fires. Technology is required to overlay imagery with labels for potential targets. Imagery can also be overlain on registered maps to give detailed coordinates. Situational awareness is also important to the dismounted warfighter as well as to a pilot. Hands-free, see through displays with wireless input and wearable computers

will provide a battlefield “augmented” reality system that will bring the individual soldier or marine into the network.

A third technology dealing with the integration and presentation of information is the development of coordinated software “agents” to manage information flow. Agents are software tools that can perform specific tasks assisting a decision maker such as integration information management, cueing and alerting, messaging, and tactical tasking.

Hyperspectral sensors

The spectral content of the emittance of an object can often give more information about its nature than its visual image, which can be altered by cover, concealment or camouflage. Spectral signatures can reveal the position of objects hours after they have been moved as well as their tracks by the thermal signature left behind on the ground. Spectral signatures are also present in the ocean and may be used to detect objects in the shallow water zone such as mines.

A Hyperspectral sensor can simultaneously measure hundreds of spectral lines, often in a single spectral band (such as 3 to 5 micrometers in the infrared). The relative strength of each of these lines gives a unique signature as to the nature and temperature of the emitting object. When coupled with other sensors, such as imaging sensors, it is possible to identify targets from decoys and pick out targets from a cluttered background.

Multifunction antennas

Network-centric warfare has exacerbated the increasing need for antennas for communications, command and control, surveillance, targeting, navigation and electronic warfare. Due to the different functionality of these emitters and receivers the requirements for frequency, power, wave form, and duty cycle has led to each system having a dedicated antenna optimized for its function. Significant technology development in wideband semiconductors leading to wideband oscillators and amplifiers coupled to developments in electronically steered arrays and digital beam forming has enabled the development of multifunction, multiband, multibeam, digital RF apertures. Shared apertures will reduce topside clutter and signature on ships and could enhance the capability of smaller platforms by adding functionality.

6. Summary

The Navy and Marine Corps are developing the operational concepts and systems to employ Network Centric Warfare across globally dispersed forces. At present, many of the tenants of NCW and its overall operational effectiveness are unproven. In particular, potential vulnerabilities need to be uncovered and addressed. Vulnerabilities can arise from two causes. The first cause is due to the very complexity of a comprehensive network. If the basis of a warfighting concept is network-centric operations then the reliability and maintenance of the network becomes the critical path to operational effectiveness. As a network becomes more complex, its behavior becomes harder to maintain and even to predict. Critics of network-centric warfare feel that too much hangs on the reliability of the network in a real operational environment and there is too much risk in a “global” verses a localized network approach. A

second vulnerability lays in the consequences of either an overt or covert attack on the network. An attack could be either directed to bring down the network or to subvert information in the network. Solutions to these concerns include physical and electronic hardening of components, redundant and self-healing network paths, and transparent to the user network-reconfiguration. Additionally extensive test and evaluation of networks are essential in realistic environments with red-teaming to uncover weaknesses. Beyond making the network more secure, elements at the edge of the network must retain a level of autonomy to continue action if the network lapses.

FORCEnet is the Navy's architecture for the implementation of NCW. In order to address potential vulnerabilities and technical shortfalls FORCEnet will proceed with an incremental implementation of systems (spiral development) as technology advances. Also, both the very rapid development and turnover of IT and the fact that most development comes from the commercial sector have significantly impacted IT acquisition mandating a spiral development approach. Because of the continual evolution in IT the FORCEnet architecture will require considerable flexibility while retaining required functionality and standards.

The naval IT program extends from basic research to acquisition, test and evaluation, and battlefield experiments. A robust information technology program is essential for the Navy and Marine Corps as Netcentric Warfare operational concepts are implemented in hardware and software systems in the coming years.

Chapter Three

Air Force Information Technology

Donald C. Daniel and Paul W. Phister, Jr.

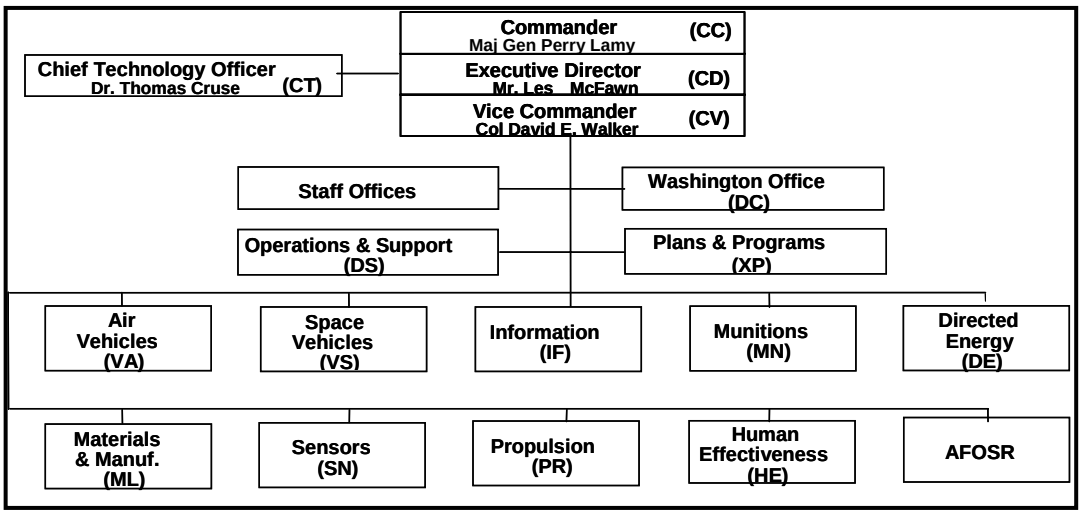
1. Introduction

This chapter focuses on Air Force information technology (IT) within the context of command, control, computer, communications, intelligence, surveillance, and reconnaissance (C4ISR).[19] The chapter reviews, at a top level, the Air Force program in information science and technology and discusses the mechanisms used to transition results into operational environments. Technical and programmatic issues associated with the activities are also discussed.

2. The Air Force Information Science and Technology Program

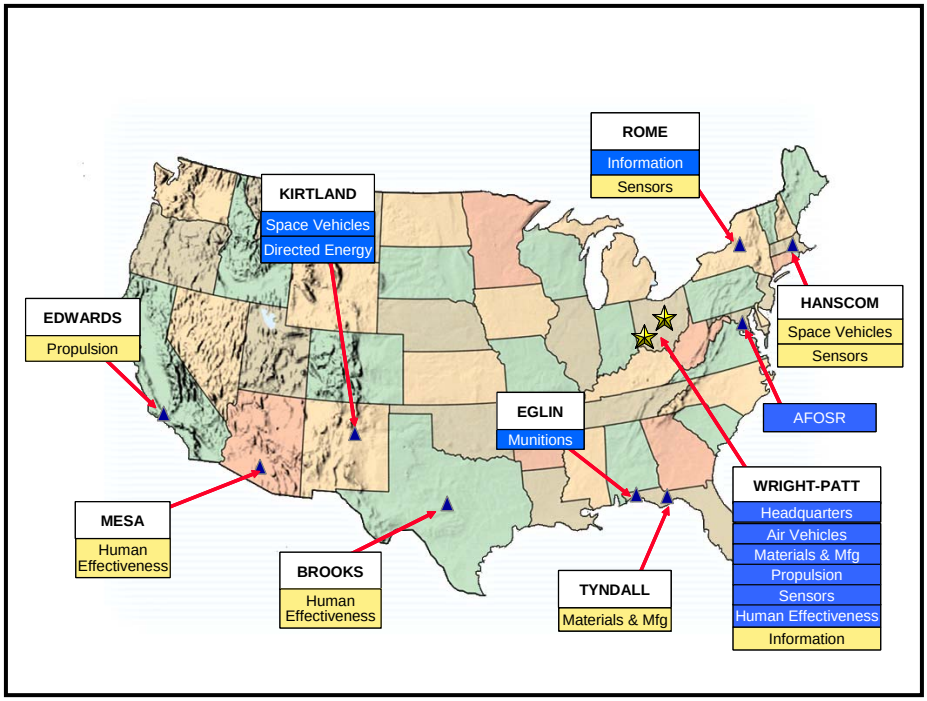
Information science and technology has been at the heart of Air Force missions since its inception in 1947. The Air Force could not complete its air-to-air and air-to-ground missions without relying upon sensors and communications systems, such as radar, thermal imaging, dedicated data links, and radio communications. The Air Force Research Laboratory (AFRL), formed in 1997, plans and executes the Air Force program in information science and technology. AFRL consists of ten technology directorates and a headquarters staff (Figure 1). AFRL headquarters and five of its directorates are located at Wright-Patterson Air Force Base (AFB), Ohio. The remaining directorate headquarters are located in Rome, New York, Washington, D.C., Eglin AFB, Florida, and Kirtland AFB, New Mexico, as shown in Figure 2.

Figure 1. Air Force Research Laboratory Organization



[19] We wish to thank all the individuals assigned to the Information Directorate of the Air Force Research Laboratory (AFRL/IF). Without their dedication and devotion to duty, we could not have written this section. Much of the information was taken from detailed briefings that reflect the strategy and vision of the members of AFRL/IF.

Figure 2: AFRL Operating Locations



Information Directorate, headquartered in Rome, N.Y., has primary responsibilities for the Air Force information science and technology program. In addition, funding for basic research in information technologies comes from the Air Force Office of Scientific Research in Washington, D.C. Where appropriate, other IT activities are also executed by elements of the AFRL Human Effectiveness Directorate and the Sensors Directorate.

The AFRL Information Directorate has a combined government civilian, military, and contractor workforce of approximately 1,400 people with a total annual budget of approximately $500 million. The organization has its roots in the former Rome Air Development Center and Rome Laboratory, which were located at the former Griffiss AFB. Following Base Realignment and Closure activities in the 1990's, the Information Directorate found itself at the same location, but in a technology and research park environment (called the Griffiss Business and Technology Park). The organization has evolved from one concerned primarily with radar and antenna technology to one focused on information science and technology, as shown in Figure 3. The majority of its financial resources are currently from non-Air Force science and technology sources with the Defense Advanced Research Projects Agency (DARPA) as the largest contributor. Due to the nature of information technologies, the focus of the Directorate is primarily near-term (1-6 years) to mid-term (7-12) years. Long-term (13-25 years) research centers on the areas of bio/nano/quantum information sciences. The science and technology program of the Information Directorate is built around seven focus areas: information exploitation, information fusion and understanding, information management, connectivity

(ground, air, space, cyber), advanced computing architectures, cyber operations, and command and control. These seven areas are in direct support of the Directorate's three thrusts, namely: Global Awareness, Global Information Enterprise, and Dynamic Planning and Execution. Software applications lie at the heart of all these activities with considerable emphasis given to man-machine and machine-machine interfaces.

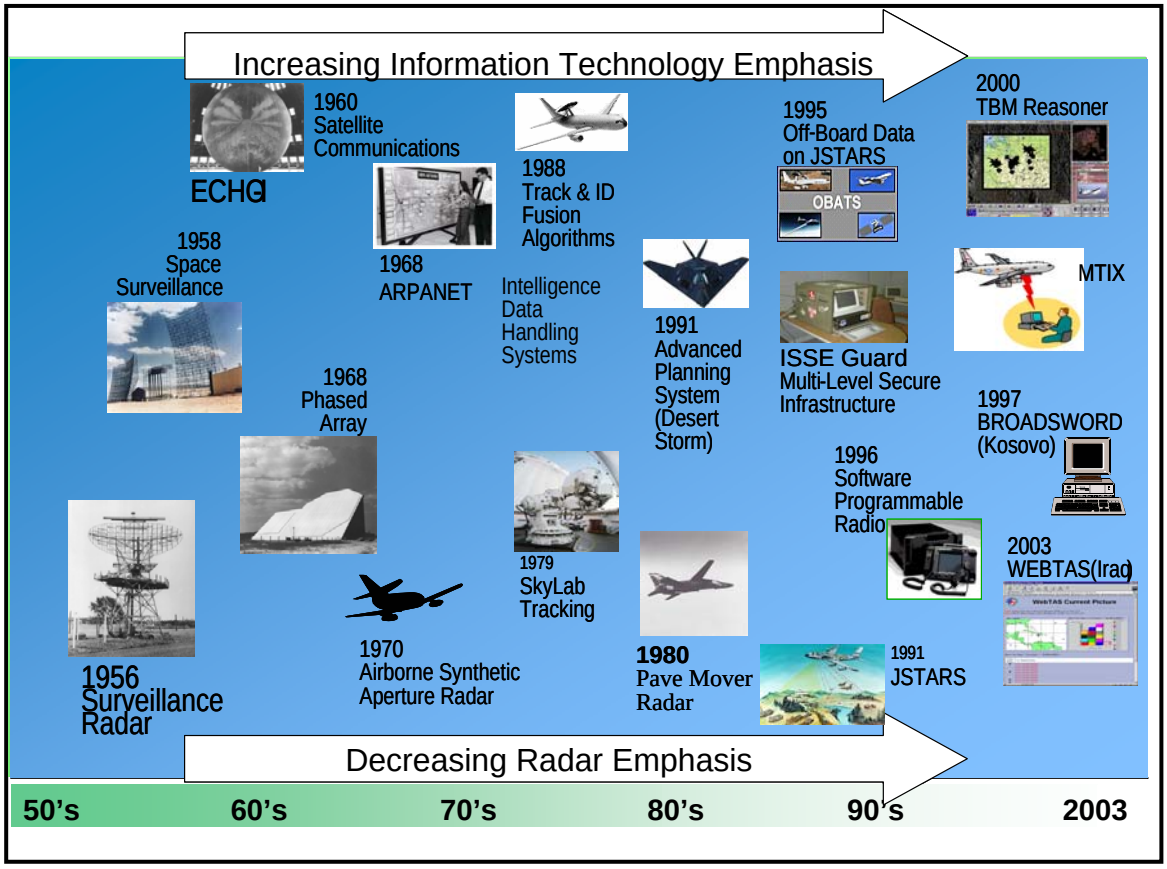


Figure 3. AFRL Information Directorate Heritage

Global Awareness is concerned with the acquisition, exploitation, fusion and reasoning of information from intelligence, surveillance, and reconnaissance data as well as open source and commercial data. Its goal is to provide consistently tailored, quality situational knowledge to decision makers at all levels of command. Fusing information from multi-sources is a critical challenge, as is archiving it for continued use. The Global Information Enterprise will interconnect all members of the Air Force via a netted communication and information system available at any time and for any task or mission. This ability to move, process, manage, and protect information is the goal of the global enterprise in supporting global awareness and dynamic planning and execution throughout the global information grid.

Reliable communications — which requires moving massive amounts of raw and processed information through a global communications grid — is fundamental to future Air Force command and control. This is especially true in the dynamic world we now face and will continue to face in the future. If one considers only the various modes of transmission used by the Global Information Enterprise, including land lines, radio frequency propagation through the

atmosphere and space, and future laser communication in space, each with its own transmission characteristics, one can begin to understand the complexity of maintaining a reliable system. Another complicating factor is the variation in level of operations, from routine to crisis-driven surges. Additionally, in the Information Age, where more and more nations have access to digital information, information assurance becomes a dominant factor in securing our systems from that of a potential adversary.

The third thrust, Dynamic Planning and Execution, is concerned with rapidly exploiting superior, consistent knowledge of the battlespace. Its goal is to conduct faster, better-informed, and more accurate decisions in complex, uncertain environments (e.g., surface, air, space and cyberspace) to shape and control the pace and phasing of engagements. To achieve these goals, the Air Force is developing the technologies and software tools required by decision makers to conduct a wide range of peacetime and wartime operations. Its focus is to allow information to be exploited for wargaming, strategy development, and operational execution. Simulation tools allow strategies to evolve via modeling and wargaming. Operational capabilities include planning, execution and management, as well as assessment of actions taken.

In support of these three thrusts, AFRL Information Directorate has focused its technology efforts into seven key areas: Information Exploitation, Information Fusion, Information Management, Advanced Computing Architectures, Cyber Operations, Air and Space Connectivity, and Command and Control. Each of these areas is described briefly below:

1) Information Exploitation involves the estimation and prediction of signal and feature states based on the characterization of and association between pixels or signals, together with the estimation and prediction of entity states on the basis of observation-to-track association, continuous state estimation (e.g. kinematics) and discrete state estimation (e.g. target type and ID).
2) Information Fusion is defined as the process of combining information (in the broadest sense) to estimate or predict the state of some aspect of the universe. The process is characterized by continuous refinement of its estimates and assessments, and by evaluation of the need for additional sources, or modification of the process itself, to achieve improved assessment of global conditions and events or battlespace awareness.
3) Information Management is the harnessing of the information resources and capabilities of an organization in order to accomplish its objectives. The challenge of Information Management in a military context is to achieve the responsiveness and flexibility of the World Wide Web with the control and predictability of traditional Command and Control (C2) Information Management Systems.
4) Advanced Computing Architectures deals with Fundamental Models of Computation along with engineering techniques for design of computing systems from the basic hardware and software to applications of theory to design. The set of data types, operations, and features of each level of computer design is called its architecture.
5) Cyber Operations is that part of information warfare that includes the following:
    a. Information Assurance comprises those measures to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation.

b. Computer Network Defense is action taken to plan and direct responses to unauthorized activity in defense of AF information systems and computer networks.
c. Computer Network Attack operations are conducted using information systems to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
d. Computer Network Exploitation operations are Intelligence, Surveillance, and Reconnaissance (ISR) functions in cyberspace that result in the ability to gather information about the adversary, their intentions, and their capabilities.
e. Assured Infrastructure Support provides capabilities to support and assure the survivability of Computer Network Defense, Computer Network Attack and Computer Network Exploitation operations

6) Connectivity (ground, air, space, cyber) is sub-divided in three areas:
   a. High Capacity Communications, covering research areas of RF optical systems, new waveforms, switching and routing, space, and efficient use of the electromagnetic spectrum.
   b. C2ISR Networking, covering development of resilient protocols for dynamic/ disadvantaged environments, access and control, adaptive end-to-end QoS, mobile security, embedded gateways, and integration with legacy systems.
   c. Enterprise Management and Control, covering management and control across AF, joint, and coalition domains in surface, air, and space operations as well as wireless information assurance.
7) Command and Control is the exercise of authority and direction by a designated commander over assigned and attached forces in the accomplishment of a mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. This area is subdivided into four main sub-areas: effects based operations, adversarial modeling, battlefield simulation, and C2 decision support.

The flagship program of the Air Force information science and technology program is the Joint Battlespace Infosphere (JBI), an activity that comes under the information management focus area. The JBI resulted from studies performed by the Air Force Scientific Advisory Board, which noted that Air Force command and control could be improved by exploiting network technology in order for information to be delivered via an appropriate interface on a soldier's handheld computer, the pilot's heads-up display, or the virtual-reality collaborative environment where many users share information and explore courses of action through simulation.[20,21] The JBI is envisioned as a combat information management system that provides individual users with the specific information required for their functional responsibilities during crisis or conflict. The current research emphasizes an open (standards based) and extensible publish/subscribe/query architecture within which legacy, evolving, and future information systems can operate. The benefit to the warfighter is that the right information can be delivered to the right place, in the

[20] *Information Management to Support the Warrior*, Report of the Air Force Scientific Advisory Board, 1998.
[21] *Building the Joint Battlespace Infosphere*, Report of the Air Force Scientific Advisory Board, 1999.

right format at the right time, so that a decision maker can act decisively. It is important to note that the JBI is not a single activity, but a family of activities that provide a framework for developing information science and technology. The framework will, in fact, produce multiple interoperable products.

Technical activities associated with the deployment of the JBI consist of software development, hardware design and evaluation to insure that users can publish information on the Infosphere, subscribe to receive information, and query information stored within the JBI. Although various technical approaches will be designed and evaluated, the emphasis in all cases is not just on standardization, but on using open-standard protocols, such as XML, and other practical, relevant commercial information technology. The aggregation, integration, and dissemination of information from distributed databases and disparate command and control systems require the development and testing of small software programs known as fuselets.

The JBI infrastructure must also be designed to allow disparate organizational units and their information systems to be connected to and disconnected from the JBI within hours.[22] All the while, the integrity of the JBI must be protected through the design, testing and integration of information assurance technology. Currently, JBI v 1.1 (core services) and v 1.2 (web services, pluggable components to dynamically configure parts of architecture) have been released. Shifting now to the human element of information technology, we find an area that perhaps does not receive the attention it deserves. In a broad sense, the Air Force has worked this area for decades[23] but typically not at the level that it now considers. Whereas in the past, research focused on a one-man-one-machine interactive model, present focus is on the massive amounts of information with which humans are confronted and the subsequent rapid decisions they must make (sometimes with life or death consequences). More attention is also being given to the fact that the human element may be operating on the ground and not in the air.[24]

The Human Effectiveness Directorate of the Air Force Research Laboratory addresses this research primarily, but in close cooperation with the Information Directorate. Areas of human effectiveness research particularly relevant to information technology include biologically-based signal processing for information operations, auditory-visual interaction, human performance modeling integration, unmanned combat aerial vehicle operator interface, real-time human engineering for unmanned combat air vehicle automation, and aerospace displays. Figure 4 and 5 provide two examples of next generation displays. Figure 4 is a program called JView, which features Java scripted visualization technologies and Figure 5 illustrates an eyepiece visualization display that could be used by Special Operations Forces. Additionally, AFRL's Crew Aiding and Information Warfare Analysis Laboratory looks at promising technologies to support the pilot, such as helmet mounted heads-up displays.

[22] It is also interesting to note that, being loosely coupled, publish-and-subscribe architectures are well suited to the ad hoc nature of coalition operations.
[23] Information received by pilots from their cockpit instrumentation being a fundamental example.
[24] This will certainly be the case as unmanned aerial vehicles and unmanned combat aerial vehicles become more prominent.

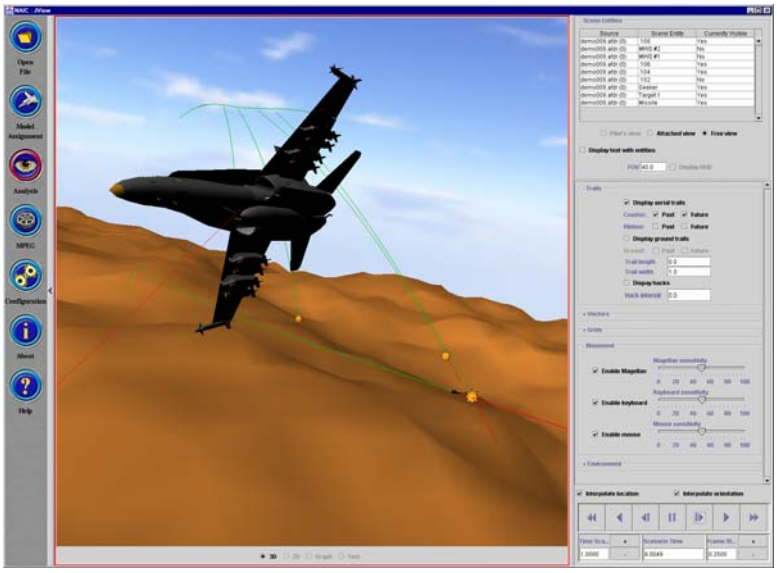


Figure 4: JVIEW

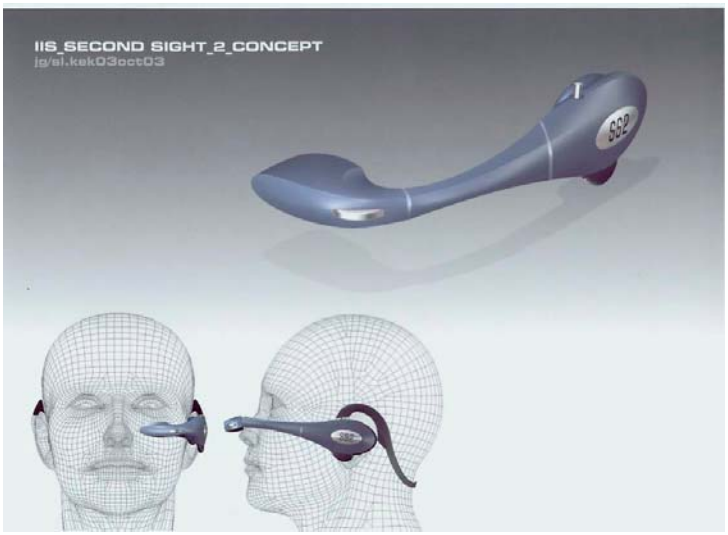


Figure 5: Head Mounted Display

Another vital element of information technology research is on the hardware and software associated with sensors used to acquire information. The importance of sensors to the Air Force is underscored by the fact that AFRL has an entire Directorate devoted to it. Sensors research covers, literally, a broad spectrum of work across the entire RF spectral band to the optical spectrum.

Extracting information from sensor data is also of critical concern, thus considerable research is conducted in sensor fusion and automatic target recognition. In the past, detection and classification of targets assumed information on a threat was collected from a single platform with a single sensor, typically an imager designed to work at a single wavelength. With hyperspectral imagers, however, it is now possible to collect high-resolution information on a threat over a broad range of wavelengths. Further, the ability to sense a threat using multiple modalities, including visible and infrared imagers, from multiple platforms, can potentially reduce the rate of false alarms. However, these new imaging modalities require the development of new target recognition algorithms. The Sensor Directorate, in conjunction with the Human Effectiveness and Information Directorates, are developing target recognition algorithms that are capable of adapting autonomously to changes in mission and threat.

A considerable amount of basic research feeds later applied research in the information technology area. This basic research includes the development of optoelectronic components for sensing and information processing, and new methods for signals communication and surveillance. The increasingly large amounts of sensor data the Air Force expects to capture in the future dictates new high-density storage technology such as optical memory as well as algorithms for information (not just data) compression. The need to detect and identify non-cooperative targets contained in these data dictates continued work in artificial intelligence, image reconstruction and enhancement, and spectral enhancement in the presence of external corruptive factors. As mentioned above, man-machine interaction is of particular interest in an information rich environment. These activities are managed by the Air Force Office of Scientific Research (AFOSR) and are executed primarily by the academic community under AFOSR sponsorship. Some basic research is also conducted by AFRL and by industry under AFOSR sponsorship.

3. Putting Information Technology to Work in the Air Force

In addition to traditional acquisition organizations such as the Electronic Systems Center at Hanscom Air Force Base, Massachusetts, the Aerospace Command and Control & Intelligence, Surveillance and Reconnaissance Center (AFC2ISRC), headquartered at Langley Air Force Base, Virginia, is vital to transitioning research results to operational users. As a Field Operating Agency of the Deputy Chief of Staff, Warfighting Integration (AF/XI), the AFC2ISRC mission is to support AF/XI initiatives to influence, integrate and improve Air Force C4ISR capabilities. The AFC2ISRC is focused on Joint Force and Joint Force Air Component Commanders' capability to dominate the battlespace and control forces.

The AFC2ISRC priorities are engaging the joint warfighter through the Joint Forces Command Joint Battle Management Command and Control Board of Directors, executing the Air Force Chief of Staff's vision of the Air and Space Operations Center (AOC) Weapons Systems, and developing and fielding the C2 Constellation. Key nodes focusing on horizontal integration within the C2 Constellation include the AOC, Distributed Common Ground System, and the E-10A Multi-sensor Command and Control Aircraft. The information superhighway, dubbed "ConstellationNet," includes ground, air, and space communications such as the Global Information Grid, the Joint Tactical Radio System, and the Multi-Platform Common Data Link.

The Center represents warfighters from all the Major Commands and provides the operational warfighter perspective to Air Force C4ISR spiral development and systems acquisition commands and processes. The Center includes the Command and Control Battlelab (C2B), the Air Force Transformation Center (AFTC), and the Air Force Experimentation Office (AFEO) which leads the planning and execution of continuous experimentation culminating with the large scale Joint Expeditionary Force Experiment (JEFX) executed bi-annually.

The Air Force Command and Control Battlelab is one of approximately half a dozen battlelabs within the Air Force. The battlelabs are small, highly focused organizations whose mission is to identify and rapidly demonstrate innovative ideas for command and control. These ideas may involve the introduction of new technology, tactics, concepts, doctrine, techniques, procedures, or all of the above. The ideas originate from different sources, including AFRL, academia, industry, and operational field organizations or within the battlelab itself. The ideas are subsequently evaluated using a variety of tools that range from modeling and simulation to the employment of forces in exercise environments. Typically, results from battlelab projects are routinely briefed to the highest levels of the Air Force. This visibility has allowed high priority capabilities to be transitioned to the warfighter in a timely manner.

Joint Expeditionary Force Experiments in the Air Force began in 1998. The goal was to allow Air Force developers to "experiment" with ideas to verify their utility to the warfighter prior to a more substantive investment. Additionally, the program allowed the warfighter to "test" new ideas to see what was in the "realm of the possible." Subsequently, three more large-scale experiments were conducted in 1999, 2000 and 2002, and more experiments are currently in process. These experiments involve a combination of live forces, simulations, and technology insertion to explore and evaluate promising new technologies and processes. Although many elements of these experiments are put to the test, two are constantly exercised: the expeditionary nature of today's Air Force and the ever-increasing requirement for information. For example, the 1998 experiment focused on the ability to move information in a distributed operation and maintain commander situational awareness while deploying fewer people and less equipment than normal. The 1999 experiment considered the integration of resources from various space organizations, as well as coalition partners. The 2000 experiment featured agile combat support (demonstrating robustness, flexibility, scalability); global transportation; time critical targeting; intelligence, surveillance and reconnaissance management; and Joint Battlespace Infosphere initiatives. The 2002 experiment looked at tactical (as opposed to strategic) control of space assets; predictive battlespace awareness (providing a capability to a commander with potential "futures" derived from possible actions of both Red and Gray forces given Blue actions); compression of the time critical target kill chain (goal of sensor to shooter in less than 10 minutes); and automated tracking and locating of U.S. and allied special operations forces; and combat rescue. The JEFX 2004 experiment is designed to "explore and empirically validate emerging concepts and capabilities that produce desired effects in the battlespace and determine implications for change related to doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMLPF)." The JEFX 06 experiment will continue the exploration of Network Centric Operations (NCO) begun in JEFX 2004.[25]

[25] Air Force Experimentation Office, "Joint Expeditionary Force Experiment (JEFX) 2004." Available online at: <http://afeo.langley.af.mil/>.

4. Issues

The Air Force is moving aggressively to address its needs in information technology. Concerns, however, remain. For example, the total AF S&T investment in all aspects of information technology is roughly $110 million per year. In addition, the Air Force receives more than twice this amount annually from other DOD activities (primarily DARPA) to execute information science and technology programs (primarily through contractors). However, even though this sounds like a formidable sum of money, this does not cover all the AF requirements in this area of science. Recently, the AF Scientific Advisory Board indicated that an additional $80 million per year would be required to adequately fund the AF S&T requirements in information technologies. Additionally, a disproportionately small amount of AF S&T funding (approximately 20 percent) is devoted to Air Force initiated basic and applied research in the AFRL Information Directorate. Less than 5 percent of the total investment supports in-house basic research at the Information Directorate.

The amount of money alone is not the issue of greatest concern. More troubling is the lack of in-house expertise in these areas. Individual scientists and engineers who actually perform research, rather than those who manage or monitor the work of industry and academia, generate in-depth expertise. Approximately 15 years ago, a hiring freeze severely handicapped the Directorate’s ability to hire scientists and engineers. This freeze was lifted five years ago, and the Information Directorate has embarked on an aggressive hiring campaign. The goal is to acquire approximately 20 new scientists and engineers per year over a five-year period and assign them to in-house research for their first five years as employees. This successful overall strategy should allow the Directorate to reach a goal of 20 percent in-house efforts.

The deficiency in basic and applied research in information technology is by itself alarming. However, it is also creating another problem — a long-term one for the Air Force. In some quarters there exists a misguided notion — based on the perception that industry is capable of introducing new technology into the market rapidly — that all work in information technology is, or should be, short-term in nature. However, one can argue that the needs of the Air Force and DOD in terms of memory, bandwidth, worldwide dispersion, speed of required action, and consequences of misinformation are sufficiently unique and so unlike any other enterprise in the world, that commercial technology alone is ill suited to address them. As the world becomes more and more dependent on information, the military's lack of long-term strategies in information technology for military applications could be catastrophic.

Joint operations also continue to be a major thrust of the U.S. military and the Air Force information technology program could improve in its efforts in interoperability at all levels discussed in this chapter. However, this same statement could be made about the other services as well. Attempting to build a truly joint science and technology framework is not an easy endeavor given the current organizational construct used by the Air Force, Army, and Navy. It is the most significant area in DOD science and technology that would benefit from the strongest possible leadership, vision, and support from the Office of the Secretary of Defense, and, simultaneously, from a similar level of coordinated support from the Air Force, Army, Navy and DARPA.

Lastly, we should continue to improve our interaction with various coalition partners in this vital area. Some progress has been made here, most notably through The Technical Cooperation Program (TTCP), which includes the United States, Australia, Canada, New Zealand, and the United Kingdom. Under United States Air Force leadership, the Command, Control, Communications and Information Systems Group of TTCP has been active in information fusion, information interfaces, space and UAV communications, networking, information assurance and defensive information warfare.

NATO's Research and Technology Organization has also addressed information technology needs for coalition operations, however, specific Air Force leadership has not been nearly as obvious here as with the TTCP. The Information Systems Technology Panel has benefited in recent years from (1) strong Canadian government and U.S. academic leadership and (2) a broad program in information warfare and assurance, information and knowledge management, communications and networks, and architectures. Specific symposia and other activities are focusing on building coalition capabilities.

It is vital that the TTCP and NATO activities discussed above promote a concept of interoperability based on roots established in their science and technology activities. There is no easier time in the life cycle of research, development, and acquisition to do this. Our scientists and engineers must become, and remain, cognizant of the long-term impact their technical approaches may have on coalition operations. Furthermore, of all subset issues associated with information technology, they should perhaps most strive for technical approaches that promote interoperability in communications.

Lastly, using information technologies for homeland defense has dramatically increased over the past four years. To this end, the Information Directorate has transitioned information technologies to Federal (e.g., the Justice Department), state and local agencies to establish a technical basis for fighting the Global War on Terrorism.

5. Summary

This chapter has presented an overview of Air Force information science and technology and how the Air Force uses one of its Centers to investigate, refine and transition these results into operations. Although the program is a significant one, it does require some improvements. Most serious of these is the need to better balance long-term and short-term research with more emphasis on the former. The program would also benefit from a much stronger in-house capability in the longer-term activities.

The program also suffers from a lack of joint activities. The framework certainly exists to accomplish this, but the level of activity needs to be increased. This holds true for both science and technology and operations. The coalition aspects of the science and technology program are adequate but they too could be improved, especially within the NATO community.

Chapter Four

The Challenge of Achieving Interoperability of Information Technology Systems

Stuart Starr and Stuart Johnson

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,[26] 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 (NCO). This vision explicitly requires substantial improvements in C^4I interoperability. To illuminate the issue, this chapter has three foci:

- characterize the nature of the interoperability problem;
- describe recent initiatives to ameliorate interoperability shortfalls; and
- 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), nongovernmental 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.

[26] Joint Vision 2020, Joint Chiefs of Staff (U.S. Government Printing Office, Washington, D.C., June 2000). Available online at: <http://www.dtic.mil/jointvision/jvpub2.htm>.

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.[27] 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 and Hayes identified four domains of warfare[28]:

- 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 and 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 and 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.[29] The LISI model also specifies five levels of interoperability (ranging from levels zero to four) as depicted in Table 1.

---

[27] Robert Nutwell and Paul Szabados, *Joint Information Interoperability: data-sharing deficiencies among the services require top-level attention,* Armed Forces Journal International, June 2002.
[28] David S. Alberts and Richard E. Hayes, *Power to the Edge*, Command and Control Research Program, ISBN 1-893723-13-5, Program, June 2003.
[29] C4ISR Architecture Working Group, *Levels of Information Systems Interoperability (LISI),* 30 March 1998. Available online at: <www.defenselink.mil/nii/org/cio/i3/lisirpt.pdf>.

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.[30]

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 (e.g., 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

[30] Mark Kasunic and William Anderson, *Measuring Systems Interoperability: Challenges and Opportunities*, SEI, CMU/SEI-2004-TN-003, April 2004.

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 U.S. 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 test bed 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. It should be noted 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.[31] 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)

[31] Annette J. Krygiel, *Behind the Wizard's Curtain*, Command and Control Research Program, ISBN 1-57906-018-8, July 1999.

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 (e.g., 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; and
- 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 U.S. 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.[32] 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.

[32] 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, National Defense University, Fort McNair, October, 9-10, 1991.

A far-reaching Department of Defense (DOD) Inspector General's report of October 17, 2002 concluded that:[33]

> 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." As discussed below, several institutional initiatives (e.g., CJCSI 3170, Management Initiative Directive (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 (e.g., 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.[34]

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

[32] *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, 17 October 2002. Available online at: <http://www.dodig.osd.mil/audit/reports/fy03/03-011.pdf>.
[34] Department of Defense Directives 5000.1 and 5000.2, 12 May 2003. Available online at: <http://hfetag.dtic.mil/dod5000.html>.

able to operate within a joint integrated architecture, subsuming operational, systems, and technical views.[35]

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 21st 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

[35] DOD Architectural Framework (DODAF) Version 1.0, 9 Feb 2004. Available online at: <http://www.defenselink.mil/nii>.

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 U.S. 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 (e.g., 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."[36] 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.

[36] *Military Operations: Recent Campaigns Benefited from Improved Communications and Technology, but Barriers to Continued Progress Remain*, GAO, June 2004.

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 stability 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, U.S. 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 U.S. 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).[37] 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 U.S., 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. This information technology driven transformation is highlighted in a series of studies issued by the Office of Force Transformation[38] 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

[37] Len Zimmermann, *Joint Methodology to Assess C4ISR Architectures (JMACA)*, Joint Test & Evaluation, brief to JFCOM J8, 12 March 2004. Available online at: <http://www.jmaca.jte.osd.mil/Documents/JFCOMJ8JMACAbrief.ppt>.

[38] See for example documents available online at: <http://www.oft.osd.mil/library/library.cfm?libcol=6>.

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," increased emphasis on the use of commercial-off-the-shelf (COTS) products in DOD, and the emergence of several industrial association initiatives.

2.5.4.1 Policy and Guidance

Several key interoperability-related policy and guidance documents have been issued over the past several years. Since many of these products are in the midst of continual revision, the following list must be regarded as a "snap shot" that is subject to substantial change in the near-term. 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."[39]
- 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.
- CJCSI 6212 entitled "Interoperability and Supportability of National Security Systems and Information Technology Systems."[40] 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.[41] The GIG is a vision for a "globally interconnected, end-to-end set of information capabilities,

[39] CJCSI 3170.01D, *Joint Capabilities Integration & Development System,* 12 March 2004. Available online at: <http://www.teao.saic.com/jfcom/ier/documents/3170_01D_12_Mar_04.pdf>.
[40] CJCSI 6212.01C, *Interoperability and Supportability of Information Technology and National Security Systems,* 20 Nov 2003.
[41] DODD 1800.1, *GIG Overarching Policy, 19* September 2002. Available online at: <www.dtic.mil/whs/directives/corres/pdf2/81001p.pdf>.

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 8320.2 entitled "Data Sharing in a Net-Centric Department of Defense,"[42] states that "Data is an essential enabler of net-centric warfare, and shall be made visible, accessible, and understandable to any potential user in the DOD as early as possible in the life cycle to support mission objectives." Key facets of this policy include organizing the data around Communities of Interest (COIs), "tagging" of all data with metadata to enable discovery by known and unanticipated users in the DOD, and posting of data to shared spaces.
- DOD Directive 4630.5, entitled "Interoperability and Supportability of Information Technology and National Security Systems,"[43] and DOD Instruction 4630.8, entitled "Procedures for Interoperability and Supportability of Information Technology and National Security Systems,"[44] introduce and discuss the concept of a Net-Ready Key Performance Parameter (NR KPP). As a key facet of this directive and instruction, it replaces the Interoperability KPP with the NR KPP. The directive states as policy that "A NR KPP, consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange." The community is still in the process of learning how to employ the concept of NR KPP to enhance system interoperability. Furthermore, the directive calls for the generation of an Information Support Plan (ISP) that serves to identify IT needs, dependencies, and interfaces to enhance the achievement of interoperability.
- The Net-Centric Operations and Warfare Reference Model (NCOW RM)[45] provides the means for acquisition PMs to describe their transition from the current to the future environment (as described in the GIG Architecture, Version 2). Note that compliance with the NCOW RM is one of four elements that comprise the NR KPP.
- The Net-Centric Checklist[46] is an evolving, capstone product, that is designed to assist PMs in understanding the net-centric attributes that their programs need to implement. The checklist is organized around the policy and guidance that is being issued in the areas of data, services, information assurance/security, and transport.

---

[42] DODD 8320.2, *Data Sharing in a Net-Centric Department of Defense,* 2 December 2004. Available online at: <www.fas.org/irp/doddir/dod/d8320_2.pdf>.

[43] DODD 4630.5, *Interoperability and Supportability of Information Technology and National Security Systems,* 11 January 2002.

[44] DODD Instruction 4630.8, *Procedures for Interoperability and Supportability of Information Technology and National Security Systems,* 30 June 2004.

[45] Net-Centric Operations and Warfare Reference Model (NCOW RM). Available online at: <http://akss.dau.mil/dag/Guidebook/IG_c7.2.1.4.asp >.

[46] Net-Centric Checklist, Version 2.1.4, OASD(NII) and DoD CIO, 30 July 2004. Available online at: <www.defenselink.mil/nii/org/cio/doc>.

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.[47] 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.[48] 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).[49] 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.[50] 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.

---

[47] *Information and Command and Control*, Aerospace America, AIAA, December 2003.
[48] *JBMC2 Roadmap Development*, Rand NDRI, March 2004. Available online at: <www.dtic.mil/ndia/2004interop/Wed/jbmc2rand.ppt>.
[49] Michael Wimbish, *New Center to help foster interoperability*, USJFCOM, 28 April 2003. Available online at: <http://www.jfcom.mil/newslink/storyarchive/2003/pa042803.htm>.
[50] Secretary of Defense William Perry, memorandum on use of COTS, 29 June 1994.

2.5.4.5 Industrial Association Initiatives

During the past several years, a number of industrial associations have begun initiatives to mitigate barriers to enhanced interoperability and net-centricity. These initiatives include the Network Centric Operations Industry Consortium (NCOIC)[51], the Net Centric Operations Industry Forum (NCOIF)[52], and the World Wide Consortium for the Grid (W2COG).[53] Furthermore, other organizations (e.g., the American Institute for Aeronautics and Astronautics (AIAA)) are in the process of formulating comparable initiatives. The following briefly characterizes the goals and objectives of a set of these initiatives:

- NCOIC. In September 2004, the 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). 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 U.S. 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.
- NCOIF. The Association for Enterprise Integration (AFEI) has established the NCOIF to help DOD systems migrate to an open business model, emphasizing the use of open standards and protocols. This initiative, begun in February 2005, has given rise to a family of working groups that are co-chaired by government and industry experts (e.g., data sharing and service strategy, IA and security, ISR, wireless and communications, architecture, and commercial acquisition practices).
- W2COG. This is an international open consortium of government, industry, and academic engineers that is seeking to advance the networking technology to support NCO. Its objective is to enhance system interoperability among organizations in a complex environment characterized by a lack of centralized authority, constant change, and incomplete technical guidance. It functions at four levels: requirements, architectures, technologies, and experiments.

Given the experience and skills of the individuals and organizations involved in these industrial association initiatives, they must be viewed as serious activities that have the potential to make a substantive contribution to key interoperability issues, particularly in the areas of systems, standards, and technology. However, given the proliferation of these industrial association initiatives, it is important to clarify their roles and relationships to ensure that they are complementary and not redundant.

[51] Network Centric Operations Industry Consortium (NCOIC). Available online at: <www.ncoic.org>.
[52] Net Centric Industry Forum (NCOIF). Available online at: <www.afei.org/news/Industry-forum.cfm>.
[53] World Wide Consortium for the Grid (W2COG). Available online at: <www.w2cog.org>.

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."[54] 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.[55] There are a total of nine Core Enterprise Services (e.g., 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.[56] 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.[57] 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

---

[54] *Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation*, (Washington, DC: Government Accountability Office, July 2004).
[55] *Net Centric Enterprise Services (NCES).* Available online at: <www.disa.mil/main/nces.html>.
[56] *Horizontal Fusion/Quantum Leap.* Available online at: <www.horizontalfusion.dtic.mil>.
[57] *Object Request Broker/Common Object Request Broker Architecture.* Available online at: <http://www.omg.org/gettingstarted/corbafaq.htm>.

maintain interoperability among fielded systems (e.g., 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 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 NR KPP 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 (e.g., 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.[58]

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).

2.5.8 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.[59] 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,

[58] Robert W. Miller, Mary Ann Malloy, Ed Masek, "Formatted Message Modernization Exploits XML Technologies," *The Edge*, Summer 2004, Volume 8, Number 1. Available online at: <www.mitre.org/edge>.
[59] *Joint National Training Capability.* Available online at: <http://www.jfcom.mil/about/fact=jntc.htm>.

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 (e.g., 6 – 12 months) for enhancing JIM interoperability.[60] 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.[61] 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.

In addition, it is notable that the major defense contractors (e.g., Boeing, Lockheed Martin, Northrop Grumman) are all in the process of creating and employing distributed testbeds that have the potential to address key residual interoperability and net-centric issues.

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 Admiral 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."[62]

[60] Coalition Warrior Interoperability Demonstration. Available online at: <http://www.cwid.js.mil/c/extranet/home>.
[61] "Joint Distributed Engineering Plant" *(JDEP).* Available online at: <http://in.disa.mil/jdep.html>.
[62] Adm. Giambastiani Slams Defense Industry, Mid-Level Procurement Officers, *Defense Today*, page 1, 5, August 2004.

In addition, the policies and guidance that govern net-centricity and interoperability are highly complex and still evolving. It will be an extremely challenging task for PMs to adhere to these policies and guidance until substantial experience has been acquired and stable, community best practices emerge.

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 releasability 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 Department of Defense is pressing on with transformation of U.S. 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.

Chapter Five

NATO Information Technologies: A New Focus on Network Enabled Capabilities

Charles L. Barry

1. Introduction

The North Atlantic Treaty Organization (NATO) approach to information technology (IT) systems is both typical of any large organization and *sui generis* because of the Alliance's multinational political and military structures. "Typical" because, like most large organizations, NATO's migration to IT applications has been no more exciting than the steady modernization of administrative processes. Today NATO uses mainly state-of-the-art IT systems and networks to facilitate its administration and management information functions. However, NATO's multinational communications and data sharing means that its many organizations and delegations must operate concurrently on a host of internal or national networks as well as on NATO common networks. Almost all Alliance organizations and delegations employ both publicly accessible web-based systems and secure systems. In an organization of 26 nations, technical and operational standards play a huge role in achieving connectivity; therefore the evolution toward newer architectures and protocols is essential and continuous.

The most unique facets of NATO IT systems relate to the breadth of Alliance political decision-making and the scope of its military operations, especially since the Cold War. All NATO political decisions are consensus decisions. Therefore, the IT systems that support consultations among NATO organizations and with 26 national capitals must be reliable, secure, rapid, networked, standardized and universal. These requirements result in an unusual level of complexity to system architectures and interface. On the military side, NATO operations are more and more information-dependent, and networks are as essential in peacetime as they are during crisis or war. As NATO's missions have changed, so have the requirements of military IT systems, with greater demand for mobile networking, address portability, and bandwidth-on-demand.

The Alliance is no operational or technological dinosaur. Far from being frozen in its Cold War birthright, NATO entered the 21st Century with slimmed down structures and new missions for responding to crises and nurturing peace and stability well beyond its members' borders. Crisis response replaced collective defense as the primary determinant of future military requirements on land, at sea, in aerospace and in cyberspace. "Battlefield" has been replaced by "battlespace" as NATO'S new operating environment, and NATO strategy now focuses on members' collective interests in addition to territorial defense. Within this context, NATO is modernizing its information technology systems by measured, regular investments in three broad areas: optimizing management information systems, creating network-enabled military capabilities, and the conduct of military information operations. In each of these areas NATO is making respectable progress in spite of its very process-oriented bureaucracy. However, much more

needs to be done before NATO IT fulfills the new requirements for crisis-related decision making and military response. Hence, pressure from NATO on members to deploy new technologies, and conversely pressure from members on NATO to agree and fund systems collectively provide sustaining influence on future investments, most of all in the application of IT to military operations.

This chapter describes NATO's progress in moving into an age of information-intensive military operations. It will point out where NATO needs greater communications and information connectivity to speed political decision-making and to facility command and control of distant multinational operations. It will highlight the key challenges to be met before NATO and its member nations reach their loftiest goal of fielding truly network enabled military forces. We will describe NATO's IT management organization and the NATO Communications and Information Systems; we will look at the Alliance's command and control operating environment and technical architectures. We will also look forward to even newer systems that appear on the horizon. Finally, we will examine how NATO can leverage its IT advances through Information Operations.

NATO is gradually coming to grips with the greater complexity, quickened decision making, mobile communications, and greater distances that define its new battlespace. NATO's Balkan experiences drove home that new missions demand far more capable communications and information systems — systems that must be scalable and upgradeable, yet durable, mobile and secure. In order to avoid an electronic Tower of Babel NATO is determined that its systems be interoperable, and that the national systems of members and operational partners include common system protocols and meet at least the minimum technical standards to communicate and share information. An array of terrestrial systems, airborne systems and space platforms are steadily being upgraded or programmed for replacement. NATO's future systems architecture must support political-military consultation among 26 NATO members and across a new military command structure that is increasingly on the move. NATO refers to this expansive and demanding connectivity portfolio as *Consultation, Command and Control*, or simply C3.

The systems that support political-military command and control and over which NATO C3 is conducted in the main, are referred to collectively as NATO's Communications and Information Systems, or CIS. NATO CIS consists of a broad array of systems as well as the policies and architecture that define how NATO land, air, and maritime forces are connected and supported. All of this vast investment must be both consistent with NATO's formal command structure design and flexible enough to facilitate changing operational concepts and new missions. It also must tie into national systems. That much NATO has accomplished or soon hopes to accomplish in the case of its newest members. However, the goal of network-enabled capabilities is still to be realized. Networks must go beyond hierarchical connections to tie in allies at many levels, and not just with NATO but between and among allies as well.

However, NATO's CIS architecture goes beyond military command and control to the facilitation of institutional management and political-military decision making. It is one seamless system in support of the overall political-military direction of the alliance. Political consultation generally occurs via modern but fixed systems. The technologies that attend the consultation function, such as system security, survivability and decision support, are common with the

technologies supporting NATO's more-mobile military systems. It should be viewed as a single system serving both civil and military nodes, even though local networks often carry out specialized functions and applications.

2. Managing and Operating NATO's IT World

NATO determines alliance-wide C3 policies, designs, and standards by consensus, based on earnest negotiations among member nations' technical experts and military users. In order to support military command and control, CIS connectivity has to reach across the whole of NATO territory and wherever forces are deployed (e.g., at sea or in the Balkans). In addition, NATO technical standards and architectures must facilitate consultations among the allies by linking NATO headquarters in Brussels to all member capitals. Parallel consultation conduits link appropriate alliance military headquarters to national military commands. These networks must handle both routine traffic and time-sensitive decision making during crises or conflict. Systems include voice, data, messaging and video teleconferencing in both secure and clear channel modes. Information and communications traffic is passed via terrestrial lines, surface-based wireless networks and satellites.

NATO CIS planners have done reasonably well since the Cold War at keeping pace with the rapid evolution in information age conduits, including use of local area networks (LANs), wide area networks (WANs), intranets and the Internet, in addition to deploying digital and optical technologies. Less successful has been NATO's efforts to get the necessary spending commitments from its members to field the systems the planners have called for. A significant portion of NATO CIS is deployed on leased or purchased commercial equipment, in particular, telephone and some satellite links. For example, a recent source selection for NATO Satcom Post-2000 leases French, Italian and United Kingdom satellites for NATO's future communications needs through 2019.

NATO CIS is overseen by the NATO Consultation, Command and Control Organization (NC3O) in Brussels. The NC3O's mission is to develop the technical architecture, standards and protocols, and overall system design from the military tactical level to the political strategic level. Since its reorganization in 1996, NC3O is managed by three interrelated entities. The NATO C3 Board (NC3B) is the senior CIS planning and policymaking body in NATO and consists of representatives of all member nations, the strategic military commands and other relevant NATO agencies. The NC3B reports directly to the North Atlantic Council (NAC) and the Defense Planning Committee, and acts as the oversight board for all NC3O activities.

The NATO C3 Agency (NC3A) carries out the policies of the Board and is the most visible day-to-day CIS operating agency. It provides objective, CIS-related scientific and technological analysis to NATO and also acts as the acquisition and procurement agent for CIS. NC3A conducts field experiments and prototyping similar to the Department of Defense's Advanced Technologies Capabilities Demonstration (ATCD) program. For example, NC3A tested the prototype of the Alliance Deployment and Movement System (ADAMS) in the mid 1990's that was used successfully in deploying forces to the Balkans. The primary customer for NC3A is Allied Command Operations in Mons, Belgium. NC3A projects are customer-funded.

The third institution under NC3O is the NATO CIS Operating and Support Agency (NACOSA), which manages, operates and controls CIS resources on behalf of users. NACOSA also provides operational support, including hardware and software maintenance, training, and associated services such as quality control over commercial and national systems used by NATO. The reorganization of NC3O was intended to accelerate the testing, experimentation, and procurement of new information technologies and systems for future command and control requirements, in particular the development of mobile networks.

When NATO military commanders identify a new capability requirement they either provide funding or seek common NATO funding by submitting a CIS Capabilities Package (CP) proposal to the NAC through NATO's Senior Resources Board and Infrastructure Committee. In fact, most CP submissions are for CIS capabilities, including urgent CIS needs for deployed forces. The NC3B approves CIS CPs from a technical and policy viewpoint, and the Military Committee prioritizes them from an operational perspective. The Military and Civil Budget Committees also get involved, depending on the type of CP. What has become apparent is that NATO's bureaucracy for processing CPs from the field is too slow for IT-related requirements and should be streamlined to be more responsive to commander's operational CIS needs.

3. The NATO CIS Operating Environment

The NATO CIS General Purpose Environment is composed of the Alliance's primary wide area and local area networks. A NATO WAN domain links fixed and mobile users into a set of common systems. User domains consist of Local Area Networks (LAN), tactical wireless communications, leased lines, and similar systems. The operating environment provides voice and data connectivity across a single fixed-mobile multi-layer network for peacetime, crisis, and conventional war. A separate, discrete Special Purpose Segment of NATO CIS is reserved for use only in a nuclear operational environment.

A primary aim of NC3A is to drive CIS investments by NATO and its members toward greater military mobility and interoperability for crisis response forces. Another high priority is to push NATO toward the use of commercial off-the-shelf (COTS) products and systems wherever possible. NC3A pursues these goals through its authority to invest in user-oriented laboratory test bedding and field prototyping, techniques that involve operational users in assessing technologies that might improve NATO operational capabilities. NC3A also uses its procurement authority to acquire and field new systems and equipment, sometimes on short notice, such as providing information systems to deployed forces. Using COTS technologies, NC3A is able to take advantage of continuous vendor-programmed upgrades and follow an evolutionary, commercial-standards acquisition strategy. NC3A is also able to be responsive to evolving C2 designs as NATO commands requirements grow. These operating principals and investment philosophy reflect a low-risk, high-yield and long-term NATO strategy for C3 interoperability.

4. Setting CIS Standards: The New NC3TA

The NC3A steers the development of NATO standardization agreements that form the foundation for future CIS interoperability. In December 2000, the alliance approved the NATO Command, Control, and Communications Technical Architecture (NC3TA). The new technical

architecture is an open-system, COTS-focused design aimed at achieving near-term interoperability requirements. For example, NC3A worked with manufacturers to promulgate NATO Standardization Agreement (STANAG) 4591 on Narrow Band Voice Coders (i.e., commercial cellular telephones that incorporate NATO-standard encryption technology). Providing industry with information such as STANAG 4591 can speed CIS interoperability. It can both define a user market and encourage manufacturers to provide the latest technology at competitive prices.

Technical standards play a crucial, if inconspicuous, role as systems are modernized or transformed. Without adherence to standards, ever more complex arrays of information systems will mean more is *worse* rather than *better*. NATO has more than 1,700 standards in nearly 1,000 agreements across all domains and has close to 300 more under development, many addressing information architectures. NC3TA identifies the services, building blocks, interfaces, standards, profiles, and related products, and it provides the technical guidelines for implementation of NATO C3 systems. These represent the minimum rules governing the specification, interaction, and interdependence of the parts of the NATO C3 system, the purpose of which is to create interoperability.

The new NATO architecture focuses on supporting standardization of information services at the boundaries between NATO Common Funded (NCF) systems and national systems. These boundary protocols can be used with partners and by members for nation-to-nation interoperability, as well as among and with NCF systems. One simple example is illustrative. NATO might specify the use of the Joint Photographic Experts Group (JPEG) file format to transmit graphics among NATO systems. However, individual nations are free to use other formats, such as Bitmap, for their internal systems so long as they employ the necessary interface protocols.

In November 2001, NATO published its plan for selection of technical services and standards that must be available at the boundaries (interface) between systems. For example, NATO mandates that Web services be exchangeable using hypertext transfer protocol, but it does not tell nations or staffs that they must use the Windows 2000 operating system. By elaborating on a minimum set of boundary services, NATO reduces the expense (and often eliminates time-consuming debates) of meeting NATO standards within a system focused on interface standards and not complete system standardization. The boundary architecture is based on the concept of a federation of fixed and mobile systems and networks that together compose a NATO intranet. The system has Internet standards and Internet protocols at its core, including the four-layer Transmission Control Protocol/Internet Protocol (TCP/IP) stack that many commercial applications (for example, e-mail) use. As the use of Internet standards and accepted protocol stacks testifies, NATO is committed to the adoption of COTS standards wherever possible. COTS-standard hardware and software remains unmodified as much as possible as it is incorporated into NATO's CIS inventory. However, off-the-shelf equipment may still be militarized to some extent, for example, by fitting tactical systems in ruggedized housings or adding military-specific software, such as enhanced security systems.

NATO's consensus decision-making process can be too tedious for reaching timely agreements on CIS standards, particularly for rapidly evolving information systems. Dramatically shortened

life cycles for new products have become the rule, not the exception. Some standards are agreed only as NC3O is near acceptance of the next system. To deal with the reality of rapid obsolescence NATO standards encompass several recent versions of most CIS systems. It also clings hard to its COTS focus – where new systems are readily available at lower cost, investing in military-specific CIS solutions only when a significant benefit can be derived and where a desired level of interoperability can be achieved. For all CIS candidate systems, NATO looks for evidence of a near-term standardization consensus and sufficient scale of application. Wherever possible, existing systems standards or open standards (i.e., COTS standards) are the default.

Nonetheless, Alliance-wide standards remain difficult to put in place, and even when they have been agreed upon, interoperability often proves elusive. Standards can be ignored by member nations or adoption can be delayed due to prohibitive cost of transition. Indeed, to achieve NATO's goal of fully interoperable Alliance-wide CIS systems, the allies will have to place higher priority on resourcing CIS in both NATO and in their own national budgets. Agencies such as NC3O will also have to keep working for solutions that make systems integration and data exchange more feasible. Software programmable hardware such as the Joint Tactical Radio System (JTRS) is one promising technology finally coming to fruition. Such systems point the way to ultimate success in the goal of interoperable NATO forces, and network-enabled command and control in the future.

5. Fielding Information Systems for the Future

In 2002, NATO began deployment of its new General-Purpose Communications Systems (NGCS). This system is replacing the obsolete NATO Integrated Communications System as the primary backbone for connectivity from the strategic military commands to NATO headquarters staffs and to Alliance member capitals for collective decision-making. The military-unique resources of NGCS support communications and information requirements from the strategic military commands down to lower level commands, and on down to both fixed sites or deployed units, such as the new NATO Response Force (NRF) or a larger Combined Joint Task Force (CJTF). As it comes on line, NGCS will provide alliance-wide operational command and control. NATO CIS must still define and deploy architectures for peer-to-peer network-enabled capabilities. That hurdle will require additional investment and should be a near term high priority. NC3O has highlighted that goal and should gain critical new support from recent decisions to organizationally relocate NC3O under the new Allied Command Transformation (ACT).

NATO's firm political consensus to engage in military missions beyond its own territory and agreement to create a new, more mobile and flexible command structure provide the foundations for investment in a new, extended CIS system to support future alliance missions. NATO's new C3 Technical Architecture provides the standards that will push investment toward transformational networks and systems. Together these initiatives define a strategy for complete command and control redesign. When they are substantially in place, NATO forces will be poised to respond to crises well beyond NATO territory and perform a wide range of military tasks, from peace operations to combat operations. Attention now shifts to the commitment of national and NATO funds for expeditious fielding of new and upgraded CIS capabilities. Some of the most critical systems and their status are described in Table 1.

Table 1. Major NATO C3 Systems supporting military Command and Control

System	Description
Allied Command Europe (ACE) Automated Command and Control Information Systems (ACCIS)	ACCIS will provide secure automated C2 support for commanders throughout Allied Command Operations. Basic services include collaborative software tools, Web services and MS Office/Windows 2000 OS. Decision support software allows exchange of a combined air, land and maritime NATO-wide operational picture. Initial fielding is was nearing completion as of this writing.
Maritime Command and Control Information System (MCCIS)	A COTS-based open architecture system optimized for maritime use, MCCIS was fielded by ACLANT and operated over all command levels with proven interoperability. MCCIS and ACCIS now serve the same strategic command and therefore should be linked.
NATO General-Purpose Communications System (NGCS)	NGCS is NATO's primary future voice and data backbone or bearer system to tie together all political and military C3 elements including NATO headquarters, military commands, deployed NRFs/CJTFs, and members' defense communications networks. NGCS deployment began in 2002 in three commercial components, including data, voice, and real-time semi-permanent bandwidth on-demand.
NATO Special-Purpose Communications System (NSCS)	A specialized bearer system for nuclear related communications.
Joint Tactical Information Distribution System (JTIDS), also called Link 16	Link 16 is a jam-resistant, spread-spectrum, secure communication identification and navigation system for automatic data and voice links among land, air and maritime forces in real time. Each terminal receives the tactical situation automatically in real time updates. Link 16 is fielded on NATO AWACS and among a few NATO member forces (US, UK, France) on tactical aircraft, ships, and land forces. Thousands of additional units are programmed by NATO allies, promising a significant boost to alliance network enabling capabilities. Although old, Link 16 is considered a key system for the future.
Crisis Response Operations in NATO Open Systems (CRONOS)	An older Windows NT Information System developed in 1996 for IFOR in Bosnia. Provides secure connectivity up to NATO Secret. Used in Bosnia, CRONOS was to be retired but is still in use in early 2005.
NATO Air Command and Control System (ACCS)	Will facilitate planning, tasking, execution and surveillance of NATO air operations, including for NRF/CJTF. Based on open system architecture and emphasizes COTS components. First level of operational capability (ACCS LOC1) due in mid-2005.

6. NATO CIS Futures

Outdated communications capabilities — legacy hardware and software, stand-alone systems, and non-interoperable national architectures — remain stubbornly in operation by many military forces and defense-related agencies at the national level, sometimes forcing NATO to maintain expensive similar systems just to preserve Alliance-wide connectivity. The main culprit remains a dearth of national investment. The pressure to acquire up-to-date C3 capabilities increased with Prague Capabilities Commitment in 2002 and was underscored again at the June 2004 NATO summit in Istanbul. As a result, more nations are beginning to respond. NATO has a good roadmap — an agreed-upon, well-defined technical architecture and a system of systems coming on line for the future. Sustained investment decisions by NATO as well as nations will achieve needed momentum and bring realities. Nations unable to invest will simply be left behind with second-rate forces.

C3 capabilities are being tested by dispersed NATO-led or supported operations in the Balkans, Mediterranean, Afghanistan and Iraq — command and control that must also extend to over the horizon response forces like the NRF and CJTFs. Right now, NATO's High Readiness Force (HRF) commands and forces are connected as hierarchical structures. The future is to network these forces at all levels using peer-to-peer means, with access to a common operational picture in which any element — ship, aircraft, ground unit, or headquarters at any echelon or component — can access real-time information about any part of the battle space. Such a network among multinational combat systems and nodes is unprecedented and far more challenging than at the national level. Fortunately, many NATO military officers and civilian leaders have experienced first hand the multiplier effects of limited networked forces in the Balkans. They are convinced that network-enabled forces are essential to meet the challenges ahead.

7. NATO Network-Enabled Capability (NNEC)

In 2004, NATO took a novel approach to funding in order to push forward a concept similar to the U.S. concept of Network-Centric Warfare (NCW). The new NATO conceptual goal is called the NATO Network Enabled Capability (NNEC). The difference between the two concepts is more one of perspective than substance. Like NCW, NNEC's aim is to network NATO military units, platforms and systems across an entire deployed force such as the NRF, as well as all the systems and organizations supporting that deployed force. When NNEC is a reality, NATO will have moved away from a traditional hierarchical operating concept and point-to-point communications, and into a concept of self-defined operational networking. The question most observers are asking is, when can we expect NATO to step up to that goal, especially with funding?

In early 2004, the allies realized that NATO's slow common funding approval process would not allow any real progress toward NNEC in less than five years. Therefore, a number of nations contributed funding for an exploratory project by NC3A, much like a venture capital initiative. By June 2004, as many as 12 allies had joined the funding group and the project's momentum remains on track. The initial deliverable — reference scenarios in which NNEC would operate — was recently completed. The other deliverables include an Interoperability Concept defining key operations and information sharing capabilities needed to support the network; Enabling

Elements that identify (or recommend) key systems outside the responsibilities of CIS that are needed to enable the NNEC and how they might be integrated; and, a NATO Roadmap, including 'quick win' investments to transform from a point-to-point communications architecture to NNEC. Of these deliverables, the headline focus is on the June 2005 Roadmap.

For NNEC to move from the drawing board to operational support in complex joint *and* combined scenarios, NATO will have to succeed in melding technical architectures, standards, doctrine, operational employment concepts, and defense investments (both NATO and national). More than eight years of research, experimentation and ad hoc networking in the Balkans, and new demands in Afghanistan, have created an apparent strong commitment among NATO allies to achieve NNEC. The NNEC initiative will be helped by NATO's already-agreed technical architecture and concept of interface standards. The next step, and most telling, will be to see hard investments that will turn concepts into real capabilities.

8. NATO and Information Operations

A full discourse on NATO and IT is not complete without an examination of Information Operations, a relatively new type of military operation (referred to by NATO as Info Ops and by the U.S. as simply IO). Just as militaries have engaged adversaries on land, sea and in aerospace, they now must conduct operations in cyberspace. Modern operations across the conflict spectrum are now critically dependent on information and IT systems. It is no longer possible to commence operations without including information operations, at least defensive operations. Capabilities that protect friendly force information and degrade or disrupt an adversary's information are important force multipliers, whether conducting peace operations, responding to crises, or fighting a war. The vulnerabilities and invulnerabilities of NATO's information systems and those of NATO's adversaries must be well understood. For that reason there must be close and continuous coordination between Info Ops planners and intelligence planners.

Info Ops includes all actions taken to affect an adversary's information and information systems while protecting NATO information and information systems. NATO or its members have been conducting Info Ops for years on an informal contingency basis. Today, the domain of Info Ops is on a par with other domains of warfare and has its own doctrine, policymaking, training, specialized capabilities, and deliberate military planning. Most operations focus on the protection of IT systems from intrusion and from the degradation of secure voice and data networks and high-speed data processing. NATO embraces the application of IT in all military functions, but in particular for command and control, intelligence (including reconnaissance and surveillance) and logistics. Nowhere will these functions by more dependent on assured secure information than in the long-range operations NATO envisages for the NRF.

At NATO HQ, Info Ops planning falls under the Operations Directorate of the International Military Staff, which promulgates policies for planning, training, doctrine development and actual operations. Planning and doctrine development is done at the strategic level (Allied Command Operations and Allied Command Transformation), and lower levels of command also engage in Info Ops planning and execution. NATO's experience with Info Ops is limited to the past several years and has focused mainly on defensive Info Ops. More needs to be done to develop emerging doctrine and capabilities. One step would be to raise the prominence of Info

Ops in exercises, focusing on intrusion detecting and conducting operations via back-up IT systems.

Broadly, NATO Info Ops fall into two categories, offensive operations and defensive operations. Offensive Info Ops degrades or disrupts an adversary's information and information systems with the aim of affecting his decision-making process. Offensive Info Ops takes advantage of an adversary's reliance on information technology for decisionmaking and coordinated operational execution. Network-dependent systems can be particularly valuable targets of Info Ops. It is vital that offensive Info Ops are closely integrated with other operational planning and with intelligence-related information systems.

Defensive operations are far more common than offensive Info Ops, and are conducted continuously even in peacetime. This ensures that information is safeguarded and that the transition to crisis response or conflict is not a period of information interruption. There have been reports that NATO networks in the Balkans during the 1990s were hacked and vulnerable to malicious viruses. Defensive Info Ops protect information systems in four ways: by protecting the information environment, through attack detection, by rapid capabilities restoration and by options for attack response. Whether offensive or defensive, Info Ops must be fully integrated into the overall campaign plan. NATO conducts Info Ops at all levels of conflict, strategic, operational and tactical, as well as across the spectrum of peacetime to crisis management and conflict resolution.

NATO Info Ops doctrine is both nascent and evolving rapidly in an effort to keep pace with operational realities, where commanders require assured information flows in order to maximize joint operational integration. NATO Info Ops policies also provide direction to national doctrines that must ultimately be synchronous with NATO for allies to cooperate and eventually be network-enabled. It is the nations that must fund Info Ops capabilities, embed NATO procedures in their training and NATO standards in their designs, and provide the resources to execute both offensive and defensive Info Ops under NATO.

9. Conclusions

Recent NATO progress is encouraging but still painfully slow in light of the fast pace IT capabilities development. A final source selection for NATO Satcom Post-2000 is to be made in 2005. At the 2004 Istanbul summit, the allies took the next step toward realizing a common funded Airborne Ground Surveillance (AGS) system by 2013. AGS, whether manned or unmanned, will be a critical information source for NATO commanders. Steady, substantial investment must be directed at fielding "reach down, reach across" interoperable connectivity, the operational embodiment of recent standards, especially interface protocol agreements. The immediate results will be to get more and more elements, units, and nodes communicating with each other. Rigorous training and exercises will reveal any gaps and limits that can be addressed and closed. Ultimately a new NNEC resource emerges that will fundamentally improve the conduct of NATO military operations.

Looking beyond the funding issue to an in-place system, the next challenges for NATO CIS will be to combine technology and operational doctrine to grapple with the unsolved internal risks of

an information-intensive operating environment. One of the most under-appreciated risks is likely to be the problem of information overload for commanders and staffs. A second emergent challenge will be preserving leader innovation in the face of information centralization at higher levels. Already we are learning of more and more centralized decision making, a situation that risks dulling of leader initiative at the tactical level.

NATO command and control has steadily adapted its structures and modernized its systems to respond to the evolution of technologies, missions and available forces since the end of the Cold War. Not least of NATO's IT accomplishments have been fielding new systems and agreeing to standards that make interoperability more, rather than less likely. The real challenges lie at the national level, where investment and convergence on new concepts for command and control—including network-enabled operations—still need more emphasis. This is not an exclusively European problem; the United States has many forces that operate outside NATO, under other regional commanders, without particular regard for adhering to NATO standards, doctrine, or interoperability. Only recently has the U.S. asserted greater emphasis on NATO interoperability in its requirements documents. However, it is clear that Europe's tasks are far more challenging in light of NATO's new crisis response missions in the Balkans, Afghanistan and perhaps Iraq. Many European nations are striving with inadequate defense budgets to slowly reorganize some of their forces for these operations, i.e., to be more mobile, deployable, and mission-flexible. Nowhere is that more critical than in the closely integrated regimes of IT and network-enabled command and control.

Acknowledgements

I am indebted to the Center for Technology and National Security Policy, its Director, Hans Binnendijk, and Senior Research Fellow, Mike Baranick, for giving me the opportunity to explore the policy dimension of military technology. I joined the Center in 2001 with 22 years of experience as an engineer, 13 of them spent on the staff of the U.S. Army Research Laboratory. The change in magnitude and scale of my work from micro-optics and nanophotonics to billion-dollar technical programs for the Army's Future Force has been professionally rewarding and, truly, a broadening experience.

The support of the Army technical community was also invaluable, most notably Dr. Tom Killion, Deputy Assistant Secretary of the Army for Research and Technology, Mr. John Miller, Director of the Army Research Laboratory, and Dr. John Pellegrino, Director of the Sensors and Electron Devices Directorate of the Army Research Laboratory. I have benefited immensely from their support over the years and especially their support of this assignment.

The most notable characteristic of the Center is the quality of its staff and the caliber of their intellect. I am humbled working so closely with individuals who have made such long lasting and significant contributions to our nation. In the interest of space, I hope that the more-prominent of the staff will excuse my not thanking them individually. I am certain that more substantial accolades than my thanks have been bestowed upon them already. However, my former officemates, Mr. Aaron Frank and Dr. Tom Hone, deserve special mention for educating me on military history, government, social science, and intelligence through many lively debates. It felt like the social science graduate school that I never had. I am similarly indebted to Ms. Leigh Caraher and Ms. Gina Cordero for many stimulating discussions.

I appreciate the efforts of my colleagues, Eli Zimet, Don Daniel, Stu Starr, Stu Johnson, and Chuck Barry, in contributing to this report. I have learned much from each of them. I also appreciate the contributions of Paul Phister. The fact that our communications have existed only in cyberspace underscores the message of this work. Finally, I appreciate the editing provided by Brad Gadberry of the American Intercontinental University in Dunwoody, Georgia. Clarity of thought and meaning reign supreme when transformational capabilities are dependent upon rapid communication, understanding, and response.

About the Authors

Charles L. Barry is a Senior Fellow at the National Defense University's Center for Technology and National Security Policy and a Washington-area consultant specializing in command and control information systems strategic management, transatlantic military relations, and defense transformation in NATO and the U.S. Department of Defense. He has lectured and published extensively on military and business affairs since 1984 as an editor, contributing author, and author of numerous books, articles, and monographs. He is presently a doctoral candidate in Public Information Management at the University of Baltimore.

Dr. Richard Chait is currently a Senior Research Fellow at the Center for Technology and National Security Policy, National Defense University. Other academic positions include Visiting Professor appointments at both Air Force Academy (2003-2004) and West Point (1983-1984). He has also held several Senior Executive Service positions, including Director of Army Research, and Chief Scientist, Army Material Command. On assignment from Carnegie Mellon University, he was also Senior Technical Advisor, Office of the Air Force Deputy Assistant Secretary for Research, Development and Engineering. Prior positions in the private sector have included the National Academy of Sciences as Director, National Materials Advisory Board, and early in his career as Staff Engineer, United States Steel Corporation. Dr. Chait has graduate degrees in Metallurgical Engineering and Solid State Science and has published over 70 open literature papers/reports and is co-editor of three books.

Dr. Donald C. Daniel is a Principal Research Engineer with the Georgia Tech Research Institute and a Distinguished Research Professor with the National Defense University's Center for Technology and National Security Policy. He is also a former Air Force Deputy Assistant Secretary for Science, Technology and Engineering and was the first Executive Director of the Air Force Research Laboratory. Throughout his career, Dr. Daniel has been involved extensively in international activities, having served on numerous NATO and other policy making panels and boards. He is currently the Chairman of NATO's Research and Technology Board.

Dr. Stuart E. Johnson is Deputy Director and a Distinguished Professor at National Defense University, where he occupies the Chair for Force Transformation Studies. He specializes in the impact of technology on defense planning and the transformation of U.S. military forces to meet the challenges of the 21st century. He served in the Office of the Secretary of Defense (PA&E) and was Director of Systems Analysis at NATO Headquarters in Brussels. He directed the International Defense programs at the RAND Corporation, overseeing a study program to support allied ministries of defense. His publications include studies on strategy and force planning, coalition operations with European allies, and the science of command and control.

Dr. Joseph N. Mait was a Senior Research Fellow at the Center for Technology and National Security Policy when this work was completed. He was on a special assignment from the U.S. Army Research Laboratory (formerly Harry Diamond Laboratories), where he has been since 1988. In addition to conducting his own research, Dr. Mait leads basic research activities in optics and photonics. He also served as the Sensors Directorate Associate for Science and

Technology. Dr. Mait is an Adjunct Associate Professor of Electrical Engineering at the University of Maryland, College Park, and a Fellow of the professional societies SPIE and OSA, as well as a senior member of IEEE.

Dr. Paul W. Phister, Jr., is currently the Air and Space Strategic Planner at the Air Force Research Laboratory's Information Directorate in Rome, New York. In this role, Dr. Phister is responsible for developing the Directorate's information technology investments portfolio for the years 2011 to 2029. Dr. Phister represents AFRL/IF on all activities relating to space and related technologies applicable to space development and operations. Dr. Phister is a recognized command and control subject matter expert and has supported the Air Force in near-, mid-, and long term command and control strategic investments. Dr. Phister spent 25 years in the military, where he has worked primarily in intelligence and space systems development and operations. Dr. Phister is a senior member of the IEEE, as well as a licensed software engineer from the State of Texas.

Albert A. **Sciarretta** is president of CNS Technologies, Inc., and conducts technology assessments as well as designs and executes operational demonstrations for an Army Research Laboratory sponsored NATO urban sensor demonstration and an Army Aberdeen Test Center (ATC) Joint distributed live-virtual-constructive test event. He has provided similar support to Defense Advanced Research Project Agency (DARPA) urban warfare experiments, an OSD Smart Sensor Web experiment, and a Defense Modeling and Simulation Office (DMSO) Joint Operations on Urban Synthetic Terrain (JOUST) demonstration. His current efforts include assisting the Defense Test Resource Management Center (DTRMC) and the Army's Battle Command, Simulation, and Experimentation Directorate (BCSED) in the development of science and technology investment strategies. He is a frequent volunteer participant in committees of The National Academies and DOD. He is a retired Army officer, whose service included operational assignments, instructing at the U.S. Military Academy, serving on an armored vehicle technology task force, and assisting the Chief Scientist, U.S. Material Command. He has a BS in General Engineering from the U.S. Military Academy, and has both an MS degree in Operations Research and an MS degree in Mechanical Engineering from Stanford University.

Dr. Stuart H. Starr is a Distinguished Research Fellow at the Center for Technology and National Security Policy and the President of The Barcroft Research Institute where he consults on national security issues, teaches courses on systems acquisition and assessment, and participates on Department of Defense science boards. His primary interest is in key issues associated with command and control, strategic planning, modeling and simulation, and the acquisition of complex systems-of-systems. He is currently working with the Center for Technology and National Security Policy at the National Defense University to identify options to enhance the utilization of commercial information technology in DOD systems. He has worked in both private industry and for the government. Dr. Starr is a frequent participant on special studies and scientific advisory boards. He is a member of the Army Science Board and participated on an Air Force Science Advisory Board summer study in 2002. He is a former National Science Foundation Fellow, a Fellow of the Military Operations Research Society, an Associate Fellow of the American Institute for Aeronautics and Astronautics, and a senior member of the IEEE. In 2004 the Military Operations Research Society awarded him the Clayton Thomas Medal for lifetime accomplishments in operations research.

Dr. Elihu Zimet is a Distinguished Research Professor at the Center for Technology and National Security Policy and is currently working on issues related to the role of technology in military transformation. As a member of the Senior Executive Service (SES), he headed the Special Programs, and subsequently, the Expeditionary Warfare Science and Technology Department at the Office of Naval Research (ONR). He directed basic research, applied research, and advanced development programs in missile, gun and directed energy weapons, aircraft, avionics and propulsion, low observable and counter-low observable technologies. He also provided technology support to the Marine Corps through his oversight of several Advanced Concept Technology Demonstrations including Cruise Missile Defense, Precision Satellite Targeting System, and Extending the Littoral Battlespace. For many years Dr. Zimet served on NATO AGAARD and RTO technology panels. He was twice awarded the Meritorious Presidential Rank Award in the SES and the Distinguished Civilian Civil Service Award.